

Commission of Inquiry
Concerning Certain Activities of the
Royal Canadian Mounted Police

Second Report — Volume 1

Freedom and Security under the Law

August, 1981

FREEDOM AND SECURITY UNDER THE LAW

AC6W



COMMISSION OF INQUIRY
CONCERNING CERTAIN ACTIVITIES OF THE
ROYAL CANADIAN MOUNTED POLICE

Second Report—Volume 1

FREEDOM AND SECURITY UNDER THE LAW

August, 1981

©Minister of Supply and Services Canada 1981

Available in Canada through

Authorized Bookstore Agents
and other bookstores

or by mail from

Canadian Government Publishing Centre
Supply and Services Canada
Ottawa, Canada, K1A 0S9

Catalogue No. CP32-37/1981-2-1E
ISBN 0-660-10951-4
ISBN 0-660-10950-6 (V. 1 and 2)

Canada: $12.00 (2 Volumes)
Other Countries: $14.40 (2 Volumes)

Price subject to change without notice

January 23, 1981

TO HIS EXCELLENCY
THE GOVERNOR IN COUNCIL

MAY IT PLEASE YOUR EXCELLENCY

We, the Commissioners appointed by Order in Council P.C. 1977-1911 dated 6th July, 1977, to inquire into and report upon certain activities of the Royal Canadian Mounted Police,

BEG TO SUBMIT TO YOUR EXCELLENCY
THIS SECOND REPORT ENTITLED:
"FREEDOM AND SECURITY UNDER THE LAW"

Mr. Justice D.C. McDonald (Chairman)



D.S. Rickerd, Q.C.



Guy Gilbert, Q.C.



le 23 janvier 1981

A SON EXCELLENCE
LE GOUVERNEUR EN CONSEIL

QU'IL PLAISE A VOTRE EXCELLENCE

Nous, les Commissaires nommés en vertu du décret du conseil C.P. 1977-1911 du 6 juillet 1977 pour faire enquête sur certaines activités de la Gendarmerie royale du Canada et faire rapport,

AVONS L'HONNEUR DE PRÉSENTER A VOTRE EXCELLENCE CE DEUXIÈME RAPPORT INTITULÉ "LA LIBERTÉ ET LA SÉCURITÉ DEVANT LA LOI"

M. le président D.C. McDonald

D.S. Rickerd, c.r.

Guy Gilbert, c.r.

FOREWORD

We wish to express our gratitude to all the members of our staff, whose names appear in Appendix "L". It is impossible here to name everyone specifically, but we feel impelled to mention certain members of our staff whose assistance was of marked importance to the success of our work.

We were fortunate throughout the life of the inquiry to have the services of our Secretary, Mr. H. R. Johnson, formerly of Edmonton and Victoria. His background as a private lawyer and his extensive knowledge of the processes of the federal government resulted in his being of help in a variety of ways above and beyond his administrative responsibilities.

The two main components of our staff were "legal" and "research". We hesitate to express specific thanks to members of one team first, in apparent precedence over the other. Only necessity makes us do so. The contribution of each group to the result was of equal importance.

Of our legal staff, we single out, for special mention, those counsel who devoted particularly long periods of time and assumed special responsibilities: our Chief Counsel, Mr. J. F. Howard, Q.C., of Toronto; Me Ross Goodwin, of Quebec City; Mr. W. A. Kelly, Q.C., of Toronto; and Me Yvon Tarte, of Ottawa.

Our excellent research staff was ably directed for more than two years by Professor Peter Russell, of the University of Toronto, and his deputy, Mr. John Graham, of Ottawa. We counted persistently on the readily available advice of our special adviser, Professor J. Ll. J. Edwards, of the University of Toronto.

As most of our work was necessarily in Ottawa, many members of our legal and research teams spent long periods of time away from their home cities. We wish to record our awareness that this physical burden extracted a heavy toll in personal terms, for which monetary reward and their interest in the subject-matter of our inquiry could not entirely compensate.

Several hundred allegations of misconduct on the part of members of the R.C.M.P. were sent to us by individuals and organizations. When we began our inquiry we knew that to investigate them we needed not only the involvement of legal counsel but also that of highly qualified investigators independent of the R.C.M.P. Thanks to the recognition by their superiors of the importance which our work would have for policing in Canada generally, we secured the services of four members of the Ontario Provincial Police, two members of the security division of the Directorate General of Intelligence and Security of the

Department of National Defence, and one member of the National Harbours Board Police. These were all men of experience and maturity, who devoted many months to their responsibilities on our behalf, conducting interviews in every province of Canada. We wish to record our particular appreciation to Commissioner H. H. Graham of the Ontario Provincial Police, to the Honourable John P. MacBeth, who was Solicitor General of Ontario when arrangements were made for the secondment of the four members of the Ontario Provincial Police, to Mr. D. N. Cassidy, head of the National Harbours Board Police, and to the Department of National Defence. We dare to express the hope that our experience in this regard has demonstrated that one police force can be investigated by members of another force without the materialization of those fears that are sometimes expressed about such a phenomenon.

Our Registrar, Mr. W. J. Brennan, brought to us a wealth of experience he had acquired with previous Commissions of Inquiry. His duties were not only those of Registrar; under his direction the administrative and clerical staff have been loyal and diligent, and cheerful even in periods of heavy pressure.

Mr. Oscar Boisjoly and his associates provided us with excellent "court reporting" services for our hearings, in both official languages. Each day's testimony was typed, reproduced, bound and in our hands by the following morning.

We wish to express our appreciation to Commissioner R. H. Simmonds, Mr. M. R. Dare, Director General of the R.C.M.P. Security Service, and the many members of the Royal Canadian Mounted Police and of departments and agencies of the Government of Canada, and to the many counsel for witnesses, whose courtesy, diligence and co-operation have helped to facilitate the execution of our complex task.

The process of preparing our Reports in final publishable form was rendered possible by our English-language editor, Mrs. Moyra Tooke, our team of translators from the Department of the Secretary of State, and our French-language editors, Messrs. Henriot Mayer and Marcel Lacourcière. Our appreciation of the subtleties of both of our official languages has been enhanced by our close work with these persons.

We have appreciated the co-operation of the provincial attorneys-general and their deputies, and of those Members of Parliament who gave us valuable advice.

Finally, we wish to express our gratitude to the numerous individuals and organizations who submitted briefs to us. We wish to assure them that their briefs were read carefully and that the ideas contained in them helped to shape the recommendations which we ultimately settled upon.

Ottawa
August 5, 1981

NOTE

All references to "Ex. —" are to exhibits filed at our hearings. Those exhibits filed *in camera* are indicated by the letter "C" in the exhibit number.

Similarly, all references to "Vol. —, p. —" are to the indicated volume and page of public testimony before the Commission, or of testimony originally given *in camera* but later made public in the volume indicated. However, if the Volume number has a "C" before it, that indicates that the testimony was given *in camera* and has not been made public.

A complete set of the transcripts of the public hearings of the Commission may be found at the following libraries:

Faculty of Law
University of Victoria
Victoria, British Columbia

Vancouver Public Library
750 Burrard Street
Vancouver, B.C.

Library
Faculty of Law
University of Alberta
Edmonton, Alberta

Library
University of Saskatchewan
Saskatoon, Saskatchewan

Davoe Library
University of Manitoba
Winnipeg, Manitoba

National Library
395 Wellington Street
Ottawa, Ontario

Library of Parliament
Ottawa, Ontario

Metropolitan Toronto Library
789 Yonge Street
Toronto, Ontario

Law Library
University of Windsor
Windsor, Ontario

Bibliothèque du Barreau
Palais de justice
12, rue St-Louis
Québec, Québec

Bibliothèque de la Ville de Montréal
Montréal, Québec

Dalhousie University Library
Halifax, Nova Scotia

TABLE OF CONTENTS

		Page
Part I	GENERAL INTRODUCTION	1
Part II	THE SECURITY SYSTEM: THE NATURE OF GOVERNMENTAL CONCERN AND INVOLVEMENT	37
Part III	PROBLEMS IN THE SYSTEM — R.C.M.P. PRACTICES AND ACTIVITIES "NOT AUTHORIZED OR PROVIDED FOR BY LAW" — INSTITUTIONALIZED WRONGDOING	95
Part IV	REASONS ADVANCED IN JUSTIFICATION OF ACTIONS "NOT AUTHORIZED OR PROVIDED FOR BY LAW"	359
Part V	A PLAN FOR THE FUTURE: ROLE, FUNCTIONS AND METHODS OF A SECURITY INTELLIGENCE AGENCY	403
Part VI	A PLAN FOR THE FUTURE: MANAGEMENT, PERSONNEL AND STRUCTURE OF A SECURITY INTELLIGENCE AGENCY	665
Part VII	A PLAN FOR THE FUTURE: SECURITY SCREENING	777
Part VIII	A PLAN FOR THE FUTURE: DIRECTION AND REVIEW OF THE SECURITY INTELLIGENCE SYSTEM	839
Part IX	ADDITIONAL LEGAL AND POLICY PROBLEMS RELATING TO THE SECURITY OF CANADA	907
Part X	THE R.C.M.P. POLICING FUNCTION: PROPOSALS FOR IMPROVING ITS LEGALITY AND PROPRIETY	955
	CONCLUSION TO THE REPORT	1055
	ANNEX 1 — ACCESS TO MEDICAL INFORMATION	1057
	MINORITY REPORT OF THE CHAIRMAN	1061
	MINORITY REPORT OF COMMISSIONER GILBERT	1063
	SUMMARY OF RECOMMENDATIONS	1067
	BIBLIOGRAPHY	1117
	APPENDICES	1145

VOLUME I

Part I: GENERAL INTRODUCTION 1

STRUCTURE AND CONTENT OF THE REPORT 3

A. How the Second Report is organized 3

B. The Commission's treatment of matters that cannot be reported publicly 6

THE ESTABLISHMENT OF THE COMMISSION 7

TERMS OF REFERENCE 13

A. General Approach 13

B. Specific interpretive rulings 17

THE WORK OF THE COMMISSION 23

A. Organization 23

B. Personnel 23

C. Work and Activities 23

D. Law Suits 28

BIOGRAPHICAL REFERENCE 31

Part II: THE SECURITY SYSTEM — THE NATURE OF GOVERNMENTAL CONCERN AND INVOLVEMENT 37

Introduction 37

Chapter 1: SECURITY AND DEMOCRACY: INTERESTS REQUIRING PROTECTION AND THREATS TO THOSE INTERESTS 39

A. The need for security 39

B. Security and the requirements of liberal democracy 43

Chapter 2: THE ORGANIZATIONAL RESPONSE BY GOVERNMENT 49

Introduction 49

A. The historical context and current structure of the Royal Canadian Mounted Police 49

B. The R.C.M.P. Security Service: historical evolution and current organization 54

C. The R.C.M.P. Security Service: current role 73

D. The R.C.M.P. "P" Directorate, Foreign Services Directorate and Emergency Response Teams: current roles 79

E. The Department of the Solicitor General 80

F. The role of other departments in security and intelligence 84

G. The role of the Cabinet and interdepartmental committees 89

Part III: PROBLEMS IN THE SYSTEM — R.C.M.P. PRACTICES AND ACTIVITIES "NOT AUTHORIZED OR PROVIDED FOR BY LAW" — INSTITUTIONALIZED WRONGDOING 95

Introduction 97

Chapter 1: IMPROPER ACTS 101

Chapter 2: SURREPTITIOUS ENTRIES — SECURITY SERVICE AND C.I.B. 103

Introduction 103

A. Nature and purpose of the practice: Security Service and C.I.B. 103

B. R.C.M.P. policies concerning surreptitious entries — Security Service and C.I.B. 109

C. Extent and prevalence of the practice of surreptitious entry.... 112

D. Legal and policy issues — Security Service and C.I.B. 118

E. Need and recommendations — brief summary 142

Appendix — Security Service: some cases of surreptitious entry for the purpose of intelligence probes 145

Chapter 3: ELECTRONIC SURVEILLANCE — SECURITY SERVICE AND C.I.B. 149

A. Origins, nature and purpose of the practice 149

B. R.C.M.P. policies concerning the practice 154

C. Extent and prevalence — Security Service and C.I.B. 161

D. Legal and policy issues 162

E. Need and recommendations — brief summary 199

Chapter 4: MAIL CHECK OPERATIONS — SECURITY SERVICE AND C.I.B. 201

A. Origin and nature of practice — Security Service and C.I.B. 201

B. R.C.M.P. policies and procedures — Security Service and C.I.B. 203

C. Extent and prevalence of the practices — Security Service and C.I.B 210

D. Legal and policy issues — Security Service and C.I.B. 213

E. Need and recommendations — brief summary 219

Chapter 5: ACCESS TO AND USE OF CONFIDENTIAL INFORMATION HELD BY THE FEDERAL GOVERNMENT — CRIMINAL INVESTIGATIONS 221

A. Origin, nature and purposes of practices 221

B. Department of National Revenue 222

C. Unemployment Insurance Commission 236

D. Other federal government departments and agencies 246

E. Need and recommendations 251

Chapter 6: ACCESS TO AND USE OF CONFIDENTIAL INFORMATION HELD BY THE FEDERAL GOVERNMENT — SECURITY SERVICE 253

A. Origin, nature, and purposes of practices 253

B. Department of National Revenue 253

C. The Unemployment Insurance Commission 261

D. Other federal government departments and agencies 264

E. Need and recommendations 265

Chapter 7: COUNTERING — SECURITY SERVICE 267

A. Nature, origin and purpose of disruptive countering measures 267

B. R.C.M.P. policies and practices 270

C. Extent and prevalence of countering measures 271

D. Legal and policy issues 273

Chapter 8: PHYSICAL SURVEILLANCE 277

A. Origins, nature and purpose of the practice 277

B. Legal issues 279

C. Need and recommendations — brief summary 292

Chapter 9: UNDERCOVER OPERATIVES 295

Introduction 295

A. Origin, nature and purpose of the practice 295

B. Legal and policy issues arising from the activities of undercover operatives 301

C. Need and recommendations — brief summary 328

Chapter 10: INTERROGATION OF SUSPECTS — C.I.B. AND SECURITY SERVICE 329

A. Criminal investigations 329

B. Security Service 340

C. Needs and recommendations — brief summary 340

Chapter 11: ACTS BEYOND THE MANDATE 341

Introduction 341

A. Government directives on surveillance on university campuses 341

B. Surveillance of legitimate political parties 348

Part IV: REASONS ADVANCED IN JUSTIFICATION OF ACTIONS NOT AUTHORIZED OR PROVIDED FOR BY LAW 359

Introduction 361

Chapter 1: LEGAL DEFENCES 363

A. Superior orders — Mistake of fact and Mistake of Law — Reliance on apparent authority — Necessity and Duress 363

B. Lack of evil intent 374

C. Interpretation Act, section 26(2) 376

D. Criminal Code, section 25(1) — "Protection of persons acting under authority" 377

E. Immunities 379

F. Authorization by ministers 393

Chapter 2: EXTENUATING CIRCUMSTANCES 397

Part V: A PLAN FOR THE FUTURE: ROLE, FUNCTIONS AND METHODS OF A SECURITY INTELLIGENCE AGENCY 403

Introduction 405

Chapter 1: FUNDAMENTAL PRINCIPLES 407

Chapter 2: A SECURITY INTELLIGENCE PLAN FOR THE FUTURE: A SUMMARY 413

A. Reasons for having a special federal agency for security intelligence 413

B. Essential characteristics of a security intelligence system 421

Chapter 3: THE SCOPE OF SECURITY INTELLIGENCE 427

Introduction 427

A. A statutory definition of security threats 427

B. Distinguishing dissent from subversion: lessons from the past 445

Chapter 4: INFORMATION COLLECTION METHODS 513

A. Basic principles 513

B. Controlling the level of investigation 514

C. Physical surveillance 529

D. Undercover operatives 536

E. Electronic surveillance 551

F. Surreptitious entry 569

G. Examining mail 574

H. Access to confidential personal information held by government 583

I. The warrant system and proposed legislation 592

Chapter 5: ANALYSIS, REPORTING, AND ADVISING FUNCTIONS 599

Introduction 599

A. Analysis 599

B. Reporting and advising 604

Chapter 6: EXECUTIVE POWERS AND PREVENTIVE ACTIVITIES 613

Introduction 613

A. Police powers 614

B. Permissible and impermissible preventive activities 614

C. Interrogation of suspects 622

Chapter 7: INTERNATIONAL DIMENSIONS 625

Introduction 625

A. Foreign operations undertaken by the security intelligence agency 626

B. Relationships with foreign agencies 632

C. Should Canada have a foreign intelligence service? 641

Chapter 8: RELATIONSHIPS WITH OTHER DEPARTMENTS, PROVINCIAL AND MUNICIPAL AUTHORITIES 647

Introduction 647

A. Relationships with other federal departments and agencies 647

B. Relationships with provincial and municipal authorities. 652

VOLUME II

Part VI: A PLAN FOR THE FUTURE: MANAGEMENT, PERSONNEL, AND STRUCTURE OF A SECURITY INTELLIGENCE AGENCY 665

Introduction 667

Chapter 1: THE HISTORICAL CONTEXT 669

A. Post World War II to the Royal Commission on Security, 1968 669

B. The Royal Commission on Security, 1968, and its aftermath 671

C. The era following the Royal Commission on Security: 1969-80 679

D. Conclusions 688

Chapter 2: MANAGEMENT AND PERSONNEL 693

Introduction 693

A. The importance of internal management 694

B. The Director General and senior management 698

C. Personnel policies 705

D. Approaches to leadership, organization, and decision-making 732

E. Legal advice 736

F. Internal auditing 739
G. Internal security 744

Chapter 3: STRUCTURE OF THE SECURITY INTELLIGENCE AGENCY: ITS LOCATION WITHIN GOVERNMENT 753

A. Our approach to the question 753
B. The case for a security intelligence organization outside of the R.C.M.P. 754
C. Reasons advanced for maintaining the status quo 760
D. Implementation of structural change 774

Part VII: A PLAN FOR THE FUTURE: SECURITY SCREENING 777

Introduction 779

Chapter 1: SCREENING OF PERSONNEL FOR PUBLIC SERVICE EMPLOYMENT 781

A. Historical background 781
B. Extent of the security clearance programme 787
C. Security clearance criteria 793
D. Security screening roles and responsibilities 797
E. Review and appeal procedures 805

Chapter 2: IMMIGRATION SECURITY SCREENING 813

A. Historical background 813
B. The extent of immigration security screening 819
C. Immigration security criteria 822
D. Role of the security intelligence agency in immigration screening 824
E. Immigration appeal procedures 825

Chapter 3: CITIZENSHIP SECURITY SCREENING 829

A. Historical background 829
B. The role of a security intelligence agency in citizenship screening 831
C. Citizenship security criteria 834
D. Appeal procedures 837

Part VIII: A PLAN FOR THE FUTURE: DIRECTION AND REVIEW OF THE SECURITY INTELLIGENCE SYSTEM 839

Introduction 841

Chapter 1: INTERNAL GOVERNMENTAL CONTROLS 845

A. Role of the Cabinet and Interdepartmental Committees 845
B. Role of the Privy Council Office and Interdepartmental Committees 847

C. Ministerial direction 856
D. Other forms of government direction and review 878

Chapter 2: EXTERNAL CONTROLS 881

Introduction 881

A. The Federal Court of Canada and the Security Appeals Tribunal 882
B. The Advisory Council on Security and Intelligence (A.C.S.I.) 883
C. The role of Parliament 891
D. Public knowledge and discussion of security matters 905

Part IX: ADDITIONAL LEGAL AND POLICY PROBLEMS RELATING TO THE SECURITY OF CANADA 907

Introduction 909

Chapter 1: NATIONAL EMERGENCIES 911

Introduction 911

A. The legal framework 911
B. Legislative reform 920
C. Internment 928
D. The role of a security intelligence agency in national emergencies 934

Chapter 2: THE OFFICIAL SECRETS ACT 939

A. Summary of First Report 939
B. Special Powers of Investigation 945
C. Other matters 946

Chapter 3: FOREIGN INTERFERENCE 947

Chapter 4: THE LAW OF SEDITION 951

Part X: THE R.C.M.P. POLICING FUNCTION: PROPOSALS FOR IMPROVING ITS LEGALITY, PROPRIETY AND CONTROL 955

Introduction 957

Chapter 1: CHANGE WITHIN THE R.C.M.P. 959

A. Basic principles 959
B. Management and personnel practices 965

Chapter 2: COMPLAINTS OF POLICE MISCONDUCT 967

A. Existing procedures for handling public complaints against the R.C.M.P. 968

B. Lodging of complaints 970

C. Investigating allegations of misconduct 977

D. Resolving allegations of misconduct 982

E. The Office of Inspector of Police Practices 985

F. The provincial role 989

Chapter 3: OBTAINING LEGAL ADVICE AND DIRECTION 995

A. Role of the Legal Branch 995

B. Glassco Commission's position 1000

C. Relationship of R.C.M.P. to provincial attorneys general 1002

Chapter 4: MINISTERIAL RESPONSIBILITY FOR THE R.C.M.P 1005

Introduction 1005

A. Principles governing ministerial responsibility and accountability for police activities. 1005

B. Minister's and Deputy Minister's roles in directing the R.C.M.P 1008

C. Relationship with provincial attorneys general 1014

Chapter 5: SOME METHODS OF CRIMINAL INVESTIGATION AND THEIR CONTROL 1017

Introduction 1017

A. A system for controlling criminal investigatory methods 1017

B. Surreptitious entries 1019

C. Electronic surveillance 1019

D. Mail covers and mail opening 1023

E. Access to confidential information 1026

F. Physical surveillance 1029

G. Undercover operatives 1030

H. Interrogation techniques 1033

CONCLUSION TO THE REPORT 1055

Annex 1: ACCESS TO MEDICAL INFORMATION 1057

MINORITY REPORT OF THE CHAIRMAN 1061

MINORITY REPORT OF COMMISSIONER GILBERT 1063

SUMMARY OF RECOMMENDATIONS 1067

BIBLIOGRAPHY 1117

APPENDICES

A. Inquiries Act 1145

B. Order-in-Council (6 July, 1977) 1149

C. Commission 1153

D. Opening statement of the Commission, December 6, 1977 1157

E. Reasons for Decision of the Commission, December 8, 1977 .. 1169

F. Reasons for Decision of the Commission, October 13, 1978 1175

G. Reasons for Decision of the Commission, July 11, 1979 1193

H. Reasons for Decision of the Commission, May 22, 1980 1195

I. Practice Direction of the Commission, June 20, 1980 1205

J. Order-in-Council (22 March, 1979) 1209

K. Order-in-Council (2 June, 1979) 1211

L. Commission Personnel 1213

M. Public Advertisement re: Notice as to submissions by members of the public 1215

N. Public Advertisment re: Motive as to termination date for receipt of allegations 1217

O. Witnesses who testified before the Commission 1219

P. Counsel who have appeared before the Commission other than Counsel for the Commission 1225

Q. Places and dates of hearings to receive briefs and persons and organizations that presented briefs at those hearings 1227

R. Formal Briefings 1229

S. Meetings with Academics 1231

T. Contracted studies and Consultants 1233

U. Organization chart of the R.C.M.P. 1235

V. Organization chart of the Security Service 1237

W. Informal meetings 1239

X. Judgment and reasons for Judgment of Mr. Justice Cattanach 1241

Y. Order of Mr. Justice Gibson 1251

Z. Reasons for Decision of the Commission, delivered on February 23, 1979 1253

PART I

GENERAL INTRODUCTION

Structure and Content of the Report	3
The Establishment of the Commission	7
Terms of Reference	13
The Work of the Commission	23
Biographical Reference	31

GENERAL INTRODUCTION
STRUCTURE AND CONTENT OF THE REPORT

1. Our full Report actually encompasses several separate reports, which we number in the order of their submission. Thus the First Report, entitled "Security and Information", was submitted on November 26, 1979. It dealt with sections 3 and 4, and certain related sections, of the Official Secrets Act.[1] It also dealt with access to government information concerning security and the administration of justice, and the release of that information, whether under "freedom of information" legislation or otherwise. In that First Report we deliberately left for future consideration other aspects of the Official Secrets Act, such as search and seizure and the interception and seizure of communications.[2] We also did not tackle in that Report the very significant task of fully defining the phrase "the security of Canada",[3] nor did we attempt a resolution of the problem of the delineation "between the legitimate 'lobbying' activities of a foreign government and the work of an agent of influence."[4] We also indicated that we would be reporting later on the overseeing and control of the government's security activities.[5] All of these subjects are dealt with in this our Second Report.

A. HOW THE SECOND REPORT IS ORGANIZED

2. In this Second Report we deal with most of the central issues requiring analysis and recommendations, and we have again divided the Report into several parts.

3. Part I is an attempt to put our work into context, through an examination of the organization of our Report, events leading to the creation of the Commission, an analysis of the terms of reference, a description of the way in which we proceeded in order to fulfill our mandate, and finally, a list of the names and positions of those who figure in our Report to allow our references to them to be placed in context.

4. Part II begins with a general analysis of the need for security — and it is here that we give our view of how the phrase "the security of Canada" should be interpreted — and continues with a detailed statement of the democratic norms which a security system ought to protect and must not violate in the

---

[1] R.S.C. 1970, ch.O-3.

[2] The Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, First Report, *Security and Information*, Ottawa, Department of Supply and Services, 1979, Foreword, Page x.

[3] *Ibid.*, paragraphs 40 and 119.

[4] *Ibid.*, paragraph 47.

[5] *Ibid.*, paragraph 100.

process. The organizational response of the government to this need is reviewed, including the relevant legislation, the current structure of the R.C.M.P., and the historical evolution and current organization of the Security Service. The current roles in the Canadian security system played by the Security Service itself, the R.C.M.P., other federal departments and agencies, the Cabinet and the interdepartmental committees are also considered.

5. Having thus examined the present system, we turn, in Part III, to a study of activities engaged in by members of the R.C.M.P. which might be described as institutionalized wrongdoings. These are examples of conduct carried on within the R.C.M.P. as a matter of practice with either direct or tacit approval by the managers of the Force. In Part III we look at general practices which we consider to be "not authorized or provided for by law" rather than particular acts which will be the subject of a separate Report. The practices which will be analyzed are: improper acts of a deceitful character, surreptitious entries, electronic surveillance, mail checks, access to and use of confidential information, countering, physical surveillance, violation of the law by undercover operatives, interrogation of suspects and acts beyond the Security Service mandate. We shall state briefly our recommendations as to whether and how certain of those practices — those which involve investigative techniques — ought to be made legal. A more detailed discussion of such recommendations will be set out in Part V and Part X.

6. In Part IV we consider the reasons advanced by the participants in the various activities to justify their conduct. We examine the legal and policy defences put forward by them with respect to any charges of misconduct which might be levelled against them, including their proposition that the pursuit of national security objectives provides, in itself, a justification for what would otherwise be acts "not authorized or provided for by law".

7. Parts V, VI, VII and VIII together, under a common heading, "A Plan for the Future", form a sort of 'manual' for a security intelligence agency. Part V, after describing the need for such an agency at the federal level, recommends the specific threats to national security with which the agency ought to be concerned, the methods it should use in collecting intelligence related to those threats, and the manner in which it ought to analyze and report that intelligence. We also discuss and make recommendations about: the powers and authority which the agency ought to have in responding to the threats; the circumstances in which it ought to be allowed to function outside Canada; and the relationships it ought to have with foreign agencies, other federal departments and agencies and provincial and municipal authorities. We also consider briefly, but make no recommendations about, the necessity or desirability of creating a Foreign Intelligence Service. After completing this study of the roles, functions and methods of the agency, we come, in Part VI, to deal with management and personnel policies it should adopt internally, and how the agency should be structured to fulfill its mandate most effectively and to avoid the problems which have arisen in the past. This analysis includes the question of where the agency ought to be located in the government structure. The recommendations in this regard are preceded by a review and critique of previous studies of the Security Service and its predecessors within the Force.

8. One of the major uses of security intelligence has been in the security screening process, especially in the areas of Public Service employment, immigration, and citizenship. In Part VII we make recommendations for a more limited, but more appropriate, role for the security intelligence agency in this field, and we make proposals for the disposition of the deleted parts of that role.

9. While Part VI outlines various control systems within the agency, Part VIII proposes a series of control systems which are external to the agency and thus beyond its direction. These include a modified role for Cabinet, a slightly revised interdepartmental committee system and changes in the system of analyzing and disseminating intelligence reports, whether produced by the security intelligence agency or by other departments and agencies. In Part VIII also, we make recommendations for significant changes in the exercise of ministerial direction over the agency and in the relationship of the agency to the responsible Minister and his deputy. The extent of control exercised by other government agencies is also examined. We then consider existing controls outside the government, including the Federal Court of Canada and Parliament, and examine the need for an independent review body for security matters, and for a revised role for Parliament.

10. The 'manual' found in Parts V, VI, VII and VIII responds partially to our mandate to advise and report regarding "policies and procedures" and "the adequacy of the laws of Canada as they apply to such policies and procedures". However, we present in Part IX further proposals with respect to changing inadequate laws. We recommend major revisions of the War Measures Act, as well as a proposed role for the security intelligence agency in situations of crisis. We also summarize the recommended changes to the Official Secrets Act contained in our First Report, and make proposals for further changes. Further, we take up another matter left in abeyance in the First Report: the extent to which activities of agents of foreign powers ought to be proscribed. Part IX concludes with an analysis of the need to legislate a clear definition of the meaning of 'sedition'.

11. Our terms of reference, in addition to directing us with respect to policies, procedures and laws in the security field, direct us generally "to advise as to any further action that [we] may deem necessary and desirable in the public interest" with respect to "activities not authorized or provided for by law". This latter direction is not confined to security matters. Part X contains our advice as to such "further action". It begins with advice on changes that ought to be made in the policies of the Force to instill and maintain in its members a respect for the law. We look at the current system within the Force for investigating and eradicating unlawful or improper activities by members, and propose a new system which includes external review. We also examine the way in which the R.C.M.P. obtains its legal advice. As with the Security Service earlier, we study ministerial direction and control of the R.C.M.P. and propose changed relationships between the Commissioner and the Minister and Deputy Minister. Part X is completed by a series of recommendations relating to methods of criminal investigation and their control. Some of them — for example, surreptitious entries, electronic surveillance, mail checks, access to

confidential information, physical surveillance, activities of undercover operatives and interrogation of suspects — will have been partially dealt with in Part III. Part X also covers fully the admissibility of evidence obtained by illegal or improper means, and entrapment.

12. We have not, in this Second Report, included our summary of the facts and applicable law relating to the various specific incidents about which we received evidence, nor have we dealt with the knowledge, approval and response of R.C.M.P. supervisors, senior officials and Ministers with respect to the investigative practices described in Part III. These will be covered in a separate Report. We also have not dealt in this Report with the many complaints received from the public alleging misconduct by members of the Force. The results of our investigations of those allegations will also be reported on separately.

B. THE COMMISSION'S TREATMENT OF MATTERS THAT CANNOT BE REPORTED PUBLICLY

13. In this Report we have identified all information obtained from sections of classified documents. In our opinion a number of these sections no longer need to be classified and could be released to the public.* On the other hand, there is considerable evidence gathered by the Commission itself which ought not to be released, on one or more of the grounds stated in the Order-in-Council setting up the Commission. In that Order-in-Council we were directed to hold our proceedings "...*in camera* in all matters relating to national security and in all other matters where [we] deem it desirable in the public interest or in the interest of the privacy of individuals involved in specific cases...". Certain matters, such as reports dealing with individuals whose conduct may have been a breach of the law, may need to be kept confidential only for the time required for decisions to be made regarding prosecution. Other matters will have to be kept secret until their release would no longer adversely affect national security, unnecessarily infringe on the privacy of individuals, or otherwise prejudice the public interest.

* Since presentation of this Report, all classified documents, or portions of them, quoted herein not previously declassified, have been declassified.

THE ESTABLISHMENT OF THE COMMISSION

14. We shall now outline briefly the events which led to the establishment of the Commission. In March 1976, Robert Samson, a former constable of the Royal Canadian Mounted Police and a member of the Security Service, testified at his own trial in Montreal on a charge arising from the bombing of a private residence in 1974. That occurrence had resulted in his discharge from the Force. At his trial he testified that he had done much worse things. When asked what he meant, he referred to the Agence de Presse Libre du Québec (A.P.L.Q.), "a break-in with... certain members of the Q.P.P. and the R.C.M.P... to take documents which were files of the most militant members [of the A.P.L.Q.] as well as other pertinent documents. The Agence de Presse Libre always had a fairly big list of Quebec leftists"[6]. (The evidence before us clearly indicates that members of the Montreal City Police were also involved in the operation.) The publication of this testimony in the press resulted in considerable public interest, and concern at the higher levels of government, especially on the part of Solicitor General Warren Allmand and Prime Minister Trudeau. The R.C.M.P. reported on the A.P.L.Q. incident to Mr. Allmand and to the Prime Minister. The setting up of a commission of inquiry was considered but was decided against because assurances were given to the Solicitor General and the Prime Minister by Commissioner Nadon and Mr. Michael Dare, Director General of the Security Service, that the A.P.L.Q. matter was an isolated incident. The facts of the incident were reported immediately to the Quebec Department of Justice by the federal government.

15. During the months following March 1976, the Quebec Department of Justice investigated the A.P.L.Q. matter. This resulted in charges being laid against three police officers, one from each of the Royal Canadian Mounted Police, the Quebec Police Force and the Montreal Urban Community Police.

16. Early in 1977 further assurances were given to the new Solicitor General, the Honourable Francis Fox, by Commissioner Nadon and a senior officer that the A.P.L.Q. matter was an isolated incident.

17. The next development arose out of the persistent attempts of two former members of the Royal Canadian Mounted Police to have their involuntary discharges from the Force reviewed by the Solicitor General. They were ex-Staff Sergeant Donald McCleery and ex-Sergeant Gilles Brunet, who had been discharged in 1973. They also lived in Montreal and had been members of the Security Service in Montreal. They took strong issue with their having been discharged, commenced litigation against the R.C.M.P., and sought to have their dismissal reviewed by the Solicitor General. Late in May 1977, they decided to try to see Mr. Fox. Mr. Fox arranged for them to see Deputy

---

[6] As reported in the *Montreal Star*, April 1, 1976.

Solicitor General Roger Tassé, and Assistant Deputy Attorney General Louis-Philippe Landry on June 6. The meeting was largely devoted to discussion of the circumstances of their discharge, but they made some allegations, of a general nature, that members of the Force had committed offences. That same day Mr. Tassé reported the conversation to Mr. Fox at one of Mr. Fox's regular weekly meetings with Commissioner Nadon, Mr. Dare, and other senior officers of the Force. Commissioner Nadon, at the meeting, said that the allegations would be investigated. According to Mr. Nadon, he told Mr. Fox and Mr. Tassé at that meeting that the information reported to the meeting by Mr. Tassé was exactly the same information that he, Nadon, had received on June 1, 1977, and that he had the allegations under investigation. It is the recollection of both Mr. Fox and Mr. Tassé, and Commissioner Simmonds, who was also present at the meeting, that there was no mention at the meeting by Mr. Nadon, or anyone else, about the R.C.M.P. already being in possession of allegations similar to, or in any way related to, those reported to the meeting by Mr. Tassé.

18. On May 26, 1977, the R.C.M.P. officer who had been charged arising out of the A.P.L.Q. matter entered a plea of guilty, as did the other accused. On June 16 he was sentenced, and received an absolute discharge. Mr. Fox then felt free to make a statement in the House of Commons, the contents of which he had been preparing for more than two weeks. In his statement he said:

> The former Solicitor General undertook in the days immediately following March 16, 1976, to discuss the matter with the Prime Minister who was told for the first time of the R.C.M.P. participation in the unlawful entry. The government seriously considered the creation of a royal commission of inquiry at that time. The government received, however, repeated and unequivocal assurances from the R.C.M.P. that the A.P.L.Q. incident was exceptional and isolated and that the directives of the R.C.M.P. to its members clearly require that all of their actions take place within the law.[7]

He also said (translation as given in Hansard):

> In a democratic society, Mr. Speaker, it is essential that those on whom, like the R.C.M.P. and the Security Service, falls the task of enforcing the law and protecting our basic liberties, can count upon the complete support of the people. This support, in return, must be based on the faith that those protecting these rights do themselves feel bound and indeed are bound by our laws in fulfilling their duties.[8]

19. Mr. Tassé had already, on June 9, written to Messrs. McCleery and Brunet asking them to give fuller particulars of the allegations they had made. This resulted in arrangements being made for a meeting, which was held in Montreal on June 23, between Messrs. McCleery and Brunet on the one hand, and Mr. Landry and Mr. Maurice Handfield of the Department of Justice on the other. Again, most of the meeting was taken up with the immediate problems of Messrs. McCleery and Brunet, but the meeting also resulted in their elaboration of the same allegations they had previously made, together with some additional ones. A number of these, if true, involved the commission

---

[7] House of Commons, *Debates*, June 17, 1977, p. 6793.

[8] *Ibid.*, p. 6795.

of offences by members of the R.C.M.P.; some of them indicated that practices which were or might be unlawful were being conducted by the R.C.M.P., while others referred to specific incidents. In a memorandum dated June 24 to Mr. Tassé, Mr. Landry described the information given to him. A copy of this memorandum was delivered to Commissioner Nadon on June 27.

20. This resulted in immediate high-level discussions in the R.C.M.P. On June 27, four senior members of the Security Service, having read Mr. Landry's memorandum, wrote a memorandum to the Director General, Mr. Dare, who spoke to Commissioner Nadon, Mr. Fox and Mr. Tassé. According to one of the senior officers of the Security Service, Superintendent Barr, they were concerned about allegations that were being made and that some of the members of the R.C.M.P. involved in some of the "problems"

> would not, from where we sat, be able to receive a fair hearing, if the process was allowed to unfold on a piecemeal basis, because of the nature of some of their duties and some responsibilities, if some of these matters, for example, wound up in Criminal Court. It would possibly be unfair, the process would not necessarily be fair to them and the entire story would not get out.

They were also concerned that:

> there was a great need to bring about some significant reform in the country and that perhaps this was the time and the opportunity to do that.

What Superintendent Barr had in mind when he said that was presumably reflected by the operative sentence in the memorandum:

> We wish here to reiterate and emphasize most strongly the need for a co-ordinated and total review of former Security Service operational techniques.

The reasons given in the memorandum were:

- concern that if criminal charges resulted from the investigation then under way in the Montreal area the publicity would cause major damage to the credibility of the Security Service;
- the public view of the Security Service would be worsened by responses on behalf of the Security Service, in Parliament, the media or in criminal court, to continuing sporadic attacks on the Service's investigative techniques by persons "who have knowledge, or think they have knowledge, of unorthodox practices";
- the "disastrous" effect on the morale and effectiveness which would flow from the singling out of individual serving members "for discipline, public criticism, or even criminal charges" when "very often it was the most talented and energetic investigators who were involved", and others would not be subject to such proceedings even though they were involved in similar activities;
- the desirability of having an impartial tribunal that would see the Security Service in a more favourable light than would the general public if cases arose one by one, sometimes in criminal proceedings;
- the need to have the activities of the Security Service examined "in the context of the time with the inherent pressures, different public attitudes and inadequate legislation" under which the activities occurred;

— that "in the calmer atmosphere of a Commission of Inquiry, it could be amply demonstrated that criminal intent or thoughts of personal gain were totally absent in members who undertook such activities";

— that "a Federal Inquiry may well have the effect of limiting the current Quebec judicial enquiry into the A.P.L.Q. affair" and that "there are indications that the Quebec Government's intentions may well exceed the simple desire to see that justice is done and the public informed";

— that if the R.C.M.P. took the initiative "we could perhaps have some influence in drafting terms of reference which could limit the enquiry to the Security Service" and so "avoid the prospect of the entire Force being subjected to the tortuous procedure and consumption of time that such investigations could impose".

21. The memorandum concluded by asserting that an inquiry would

> give us the time and the opportunity to present a broad detailed explanation of our operating procedures, properly set in a historical context and illustrating an inadequate working mandate

and that

> these conditions forced many totally loyal and dedicated members to resort to methods which were at least unorthodox and often bordering on illegality to carry out the duties required of them by the Canadian people. It is only by having the opportunity to present this picture in its entirety that we can hope in any way to define these actions.

22. Superintendent Barr explained to us that in expressing the hope that the inquiry could be limited to the Security Service, he was not aware that the same problems existed on the criminal investigation side of the Force (Vol. 198, p. 29189). Very shortly thereafter Commissioner Nadon asked the Solicitor General to have a commission of inquiry appointed under the Inquiries Act. The result was our appointment on July 6. In the House of Commons, Mr. Fox, announcing the appointment, said:

> Since making my statement in the House concerning the A.P.L.Q. incident, allegations have been made that members of the R.C.M.P., and more particularly members of the security service, have, on other occasions, been involved in unlawful actions in the discharge of their duties. The A.P.L.Q. incident, according to those who made the allegations, was not of an isolated and exceptional character.
>
> These allegations received our immediate attention. At my request, the deputy Solicitor General of Canada and the assistant Attorney General, criminal law, personally met with some of the individuals who made these allegations. In addition, I asked the Commissioner of the R.C.M.P. to undertake the investigations which were warranted. He later informed me, after having made preliminary inquiries, that some of these allegations might well have some basis in fact. According to the Commissioner, it would appear that some members of the R.C.M.P. in the discharge of their responsibility to protect national security could well have used methods or could have been involved in actions which were neither authorized nor provided for by law. As a result, the Commissioner has modified his position and has recommended that the government establish a commission of inquiry into the operations and the policies of the R.C.M.P. security service, on a national basis.

In the circumstances, Mr. Speaker, and considering these new developments, the government has decided to establish an inquiry commission composed of three members who will be responsible for determining the scope and frequency of inquiry practices and other activities which are not permitted or provided for in the law, involving members of the R.C.M.P., and for examining the policies and procedures regulating R.C.M.P. activities in their task, which consists in protecting the country and ensuring its security.[9]

The following passage was delivered in French. The translation is by Hansard:

... beyond particular incidents which might be brought before the commission, it is important to think about the lessons to be learned for the future. That is why the government has asked the commission's advice in terms of policies and procedures that govern or should govern R.C.M.P. activities in the accomplishment of their task, namely to see to the protection and the security of the country, of necessary mechanisms for implementing these policies and procedures, and finally of the amendments to the legislation which could be necessary, in keeping with the security requirements of our country.

Even if the commission is particularly requested to inquire into matters related to the security service of the R.C.M.P., the government has also requested to have brought to its attention any incident involving illegal action on the part of R.C.M.P. members, outside of security service operations. Regular police operations are more immediately submitted to the control and surveillance of the courts. Nevertheless, the government prefers not to restrict the terms of reference of the commission to the security service, so that eventually it could know about incidents involving unlawful acts that could be drawn to the attention of the commission. Thus, the government will be able to take the necessary steps at the appropriate time.[10]

23. Robert Simmonds became Commissioner of the R.C.M.P. on September 1, 1977, almost at the same time as this Commission was established. Before that, since 1976, he had been the Deputy Commissioner responsible for administration, and his brief time in that position was his only prior experience at Headquarters; all his earlier career, from the time he joined the R.C.M.P. in 1947, was spent in Alberta and B.C. Managing a police force the size of the R.C.M.P. is a difficult task at the best of times. Commissioner Simmonds' burden has been increased greatly during the past three and one-half years by the activities of our Inquiry and those of the provincial Inquiries. His stance *vis-à-vis* this Commission has been, throughout, one of total co-operation. We are conscious of the fact that he has put 'on hold' certain plans and proposals that he had for change within the Force, pending receipt of our Report, and also that he has felt constrained to suspend or terminate certain practices merely because to continue them *might* have meant to continue unlawful conduct. Our Inquiry and Report touch only occasionally upon Commissioner Simmonds. He inherited the situation which led to our Inquiry and participated in neither the formulation nor the continuation of the policies which have been its substance.

---

[9] *Ibid.*, July 6, 1977, p. 7365.
[10] *Ibid.*, pp. 7365-6.

THE TERMS OF REFERENCE

A. GENERAL APPROACH

24. The legal framework within which our Commission has operated consists of a specific 'Commission' issued pursuant to an Order-in-Council, the relevant provisions of the Inquiries Act together with judicial decisions interpreting it, and the laws of procedure and evidence generally applied to commissions of inquiry. Throughout our work, rarely has a week gone by in which we have not addressed ourselves to the language of our 'Commission' and sought to interpret it as a guide to resolving an issue.

25. The Commissioners appointed to any Inquiry must arrive at their own interpretation of their mandate so as to determine its true intent. It is then their task to direct the course of the Inquiry towards realizing that interpretation. They are not at liberty to inquire into matters beyond those specified by their authority, nor to adopt procedures other than those set out in their terms of reference, yet they must interpret their mandate broadly enough to avoid so rigid a construction of its language that its intent would be frustrated. This chapter is an attempt to convey the essence of our interpretation — as it has evolved over the past three years — of the language of the Order-in-Council that established our Commission.

26. Basic to our interpretation, it will be seen, is our adherence to the core element that has guided our procedural decisions — that a tribunal such as our Commission of Inquiry is created to restore public trust in a public institution which has fallen under suspicion. It was this belief that led us to conclude that as a general rule only public hearings would engender public confidence in our findings.

27. The Commission for an Inquiry such as ours is issued by the Governor in Council pursuant to the authority granted by Part I of the Inquiries Act (reproduced as Appendix A). The specific authority to issue our 'Commission' is contained in Order-in-Council P.C. 1977-1911, passed on July 6, 1977 and tabled in the House of Commons that same day. The Commission under the Great Seal is our governing instrument. Our terms of reference — what we are to inquire into — are found in paragraphs (a), (b) and (c). The remainder of the text consists of procedural directions as to how the Inquiry is to be conducted. Although the entirety of the Order-in-Council is reproduced in Appendix B, and our 'Commission' is reproduced in Appendix C, for ease of reference we reproduce here the preamble and the terms of reference.

> WHEREAS it has been established that certain persons who were members of the R.C.M.P. at the time did, on or about October 7, 1972, take part jointly with persons who were then members of la Sûreté du Québec and la Police de Montréal in the entry of premises located at 3459

St. Hubert Street, Montreal, in the search of those premises for property contained therein, and in the removal of documents from those premises, without lawful authority to do so;

AND WHEREAS allegations have recently been made that certain persons who were members of the R.C.M.P. at the time may have been involved on other occasions in investigative actions or other activities that were not authorized or provided for by law;

AND WHEREAS, after having made inquiries into these allegations at the instance of the Government, the Commissioner of the R.C.M.P. now advises that there are indications that certain persons who were members of the R.C.M.P. may indeed have been involved in investigative actions or other activities that were not authorized or provided for by law, and that as a consequence, the Commissioner believes that in the circumstances it would be in the best interests of the R.C.M.P. that a Commission of Inquiry be set up to look into the operations and policies of the Security Service on a national basis;

AND WHEREAS public support of the R.C.M.P. in the discharge of its responsibility to protect the security of Canada is dependent on trust in the policies and procedures governing its activities;

AND WHEREAS the maintenance of that trust requires that full inquiry be made into the extent and prevalence of investigative practices or other activities involving members of the Royal Canadian Mounted Police that are not authorized or provided for by law.

THEREFORE, the Committee of the Privy Council, on the recommendation of the Prime Minister, advise that, pursuant to the Inquiries Act, a Commission do issue under the Great Seal of Canada, appointing

Mr. Justice David C. McDonald
of Edmonton, Alberta

Mr. Donald S. Rickerd
of Toronto, Ontario

Mr. Guy Gilbert
of Montreal, Quebec

to be Commissioners under Part I of the Inquiries Act:

(a) to conduct such investigations as in the opinion of the Commissioners are necessary to determine the extent and prevalence of investigative practices or other activities involving members of the R.C.M.P. that are not authorized or provided for by law and, in this regard, to inquire into the relevant policies and procedures that govern the activities of the R.C.M.P. in the discharge of its responsibility to protect the security of Canada;

(b) to report the facts relating to any investigative action or other activity involving persons who were members of the R.C.M.P. that was not authorized or provided for by law as may be established before the Commission, and to advise as to any further action that the Commissioners may deem necessary and desirable in the public interest; and

(c) to advise and make such report as the Commissioners deem necessary and desirable in the interest of Canada, regarding the policies and procedures governing the activities of the R.C.M.P. in the discharge of its responsibility to protect the security of Canada, the means to

implement such policies and procedures, as well as the adequacy of the laws of Canada as they apply to such policies and procedures, having regard to the needs of the security of Canada.

The need for trust

28. The most important word in the Commission governing this Inquiry is "trust". No police force protecting the peace can be effective unless it has the trust of the people it seeks to protect; no security intelligence agency can be effective without the trust of citizens. Moreover, neither can be effective without the trust of government.

29. Our mandate stresses the role of the R.C.M.P. in protecting the security of Canada. It correctly notes that unless the R.C.M.P. has and deserves the trust of Canadians, it cannot perform that task effectively. Without the full co-operation of citizens, confident that the task is being performed competently and lawfully and with due regard for the freedom of the individual, it will not receive from government the material support which it needs, whether for its work collecting security intelligence or its law enforcement duties.

Policy and procedures and the adequacy of laws

30. Paragraph (c) of our terms of reference requires us to advise and report regarding "the adequacy of the laws of Canada as they apply to" the "policies and procedures governing the activities of the R.C.M.P. in the discharge of its responsibility to protect the security of Canada". The Concise Oxford Dictionary defines "adequate" as "proportionate (to the requirements)". Therefore, when considering the various investigative techniques and processes that the law at present makes available to the R.C.M.P. Security Service, we have asked ourselves in each instance whether the law is clearly stated, whether it deals fully with the subject and whether it provides too little or too much power, in relation to the need to protect the security of Canada.

31. One of the concerns that "adequacy" invokes is essentially the need for laws, policies and procedures that ensure that the Security Service is effective. Therefore, we have examined what the functions of a security intelligence organization should be, and what kinds of people and structure would be required in order to carry out that work effectively. It is difficult not to approach this aspect of our task as if it were separate from that part of our terms of reference which requires us to investigate and report the facts of, and the extent and prevalence of, activities involving members or past members of the R.C.M.P. that were not authorized or provided for by law. Those words apply to both the criminal investigation and security service work of the R.C.M.P. As we bring many of the strands together in this Report, we have attempted to surmount this difficulty, for the heart and soul of the concern expressed in our mandate is the importance of ensuring that, in the future, conditions will exist that will justify public trust in the R.C.M.P.

32. In making our recommendations for the future, therefore, we have not only constantly asked ourselves what powers are absolutely necessary to ensure that the work of a security intelligence organization is effective. We have also,

to balance this, searched for methods, within and outside the organization, which will enhance the likelihood that its personnel will respect the rule of law, the right of dissent, and the duty of accountability, but which will not strangle the organization's legitimate efforts.

The historical period

33. In inquiring into activities "not authorized or provided for by law" we have not, as a general rule, tried to investigate practices preceding 1969. Keeping to the past decade has not always been possible since the history of several of the practices we shall report on begins in earlier years. We, however, felt that some realistic time limit had to be placed upon our review of the past. 1969 seemed appropriate as that year saw the publication of the Report of the Royal Commission on Security, the appointment of a new Commissioner, the appointment of the first civilian Director of Security and Intelligence, and (at roughly that time) a perception by the R.C.M.P. of new international and domestic terrorist threats as well as new domestic threats of subversion arising from the separatist movement in Quebec and other movements across the country. Another reason was that any inquiry into an earlier period was likely to be frustrated by poor memories or the unavailability of witnesses. Finally, it seemed to us that the past decade was roughly the relevant period to determine the extent to which activities "not authorized or provided for by law" existed which might damage *present* public trust and confidence in the R.C.M.P.

34. However, we did not consciously limit, by time, our inquiry into the policies and procedures of the R.C.M.P. called for in paragraphs (a) and (c), especially in our research among R.C.M.P. files. In our intensive analyses of such topics as management and personnel policies in the R.C.M.P. (particularly as they have affected the Security Service), its relationship with the Solicitor General and the Prime Minister and other departments of government, the committee system, and the relationship of the R.C.M.P. Security Service with foreign agencies, our inquiry frequently took us back several decades.

The rights of witnesses

35. In conducting our inquiry, particularly at hearings at which evidence has been received under oath, we have been conscious of the importance of exercising with care the broad powers given to us, especially the power to compel a witness to give evidence as to his own misconduct. In a court of law, in a criminal trial, the accused in our system cannot be compelled to testify. However, a Commission of Inquiry may subpoena the same person, and may compel him to answer incriminating questions, although, by virtue of the Canada Evidence Act,[11] his answers cannot be used against him in a subsequent prosecution if he has objected to answering and he is compelled by the Commissioners to answer. A Commission of Inquiry has the same powers as a court to compel attendance of persons as witnesses and the production of documents, so long as the testimony and documents are relevant to the terms of reference of the Inquiry. Yet, unlike proceedings in a court of law, where an

[11] R.S.C. 1970, ch.E-10, sec.5.

indictment or summons defines the charge, an Inquiry has no need to justify the subpoena of a person or of documents by a particularized written definition of the issues. Where suspicion of wrongdoing is among the reasons for the Inquiry, witnesses can be exposed to public comment without the protection that, in the case of a prosecution, would be afforded by the law of contempt of court. These powers given to Commissioners are extraordinary powers, which Parliament has decided should be available for use when the executive considers that no other means of investigation of facts appears to be effective.

36. In preparing our First Report and this Report on laws, policies and procedures, and subsequent Reports on the activities of individuals, we have approached the issues of fact not as angels of vengeance but as dispassionate inquirers after the truth. Our task has been, not to destroy an institution or inflict wounds on its members or on public servants or persons elected to public office, but to suggest the means by which trust in an institution may be restored on the basis of truth about the past and justice for its members.

B. SPECIFIC INTERPRETATIVE RULINGS

37. We turn now from reflections on the essence of the Order-in-Council as interpreted by us, to a summary of some of the specific interpretative rulings which we have made publicly, together with supplementary remarks. This summary refers mainly to decisions that affected the scope of the inquiry rather than decisions as to procedure.

"...Not authorized or provided for by Law..."

38. In our opening statement on December 6, 1977 (Appendix D), we stated that the words "not authorized or provided for by law" directed us to inquire into and report on acts which were offences under the Criminal Code or under other federal or provincial statutes, or were wrong in the eyes of the law of tort in the common law provinces or of the law of delict in Quebec. We stated also that in interpreting those words we did not intend to ignore the moral and ethical implications of police investigative procedures.

39. Also in our opening statement we pointed out that those words required us to examine the legislative and constitutional basis for the existence of the R.C.M.P. generally, and for the existence of the Security Service of the R.C.M.P. in particular.

40. In reasons for decision pronounced on May 22, 1980 (Appendix H), we added that those words also require us to examine whether a particular act or practice, even if not an offence or civil wrong, was nevertheless beyond the statutory authority of the R.C.M.P., or was itself not authorized by normal procedures within the R.C.M.P.

41. In our opening statement we stated that in our report of a particular allegation we would give our view as to whether the conduct established by the evidence constituted an action or activity "not authorized or provided for by law". We confirmed that position in the reasons for decision dated May 22, 1980, but noted that our functions were not those of a court of law and that we

could not render a judgment of acquittal or conviction. We stated that the duty imposed upon us to "report" facts that disclose an activity which was "not authorized or provided for by law" could not be performed unless we undertook an analysis as to whether the facts, *as disclosed by the evidence before us*, constituted an offence or a civil wrong or in some other way conduct "not authorized or provided for by law". At the same time, we recognized that, in situations where there is evidence as to the acts of specific individuals in specific cases, a dilemma arises as to how we can "report" publicly, including a commentary on the legal status of the acts as it appears on the evidence before us, without causing unfairness or the appearance of unfairness to any such individual if he is then tried on a criminal or other charge after all the publicity that the report may be given. In our separate Report on activities in which there is such evidence of specific cases we shall face this dilemma. It does not require further comment here. However, we might say that in a Practice Directive dated June 20, 1980 (Appendix I), we attempted to reduce the scope of the dilemma by directing that legal submissions concerning such cases where there is evidence about individuals (as compared with cases where there is merely evidence about general practices) be given to us in private.

"...The relevant policies and procedures..."

42. In our opening statement we interpreted the words of part of paragraph (a) ("to inquire into the relevant policies and procedures that govern the activities of the R.C.M.P. in the discharge of its responsibility to protect the security of Canada") and the entirety of paragraph (c) of our terms of reference as requiring us to determine what have been and are the controls exercised by federal or provincial Ministers over the R.C.M.P. Security Service, and what methods and channels have been used by the R.C.M.P. Security Service to report and account to federal and provincial Ministers.

"...The security of Canada..."

43. In our opening statement we interpreted paragraph (c) of our terms of reference as requiring us to consider what the needs of the security of Canada are, how those needs should be protected effectively in terms of investigative work, and how that protection can be achieved in a democracy which cherishes liberty.

"...Activities of the R.C.M.P...."

44. In reasons for decision delivered on October 13, 1978 (Appendix F) concerning the Commission's procedure in regard to certain classes of 'government documents', we noted that the preamble in the Order-in-Council referred to the need for a full inquiry into "the extent and prevalence of investigative practices or other activities involving members of the Royal Canadian Mounted Police that are not authorized or provided for by law" so as to maintain public trust "in the policies and procedures governing its activities" without which there cannot be full public support of the R.C.M.P. "in the discharge of its responsibility to protect the security of Canada". We inferred from this language that our inquiry into "policies and procedures" governing the activities of the R.C.M.P. was not limited to the policies and procedures governing

the Security Service, for there can be public support for the work of the Security Service (so long as it is within the R.C.M.P.) only if there is public trust in the policies and procedures governing all activities of the R.C.M.P. We should note here that we have not in fact inquired into *all* the policies and procedures governing the R.C.M.P. However, when a policy of the R.C.M.P. has given rise to concern, the fact that it does not relate directly to the Security Service has not been regarded as a reason for refusing to examine it.

The involvement of Ministers

45. In the reasons of October 13, 1978, we concluded that our duty to report on the facts "relating to any investigative action or other activity" involving "members of the R.C.M.P. that was not authorized or provided for by law" might result in our reporting "whether members of the R.C.M.P. who, in our opinion, have, or might be held in a court to have, committed a wrongful act, were doing so upon the direction or with the consent or at least without the disapproval of a Minister of the Crown, for that might be a fact which any Attorney General might consider relevant to the process of his deciding whether or not to prosecute the members of the R.C.M.P.". We added that our Report would be incomplete as to relevant facts, and unfair to any members of the R.C.M.P. against whom in our Report we might make a "charge of misconduct" (to use the language of section 13 of the Inquiries Act) and who might otherwise feel that facts tending to exonerate them had not been brought to light, unless we inquired into and reported on the extent to which such members had express or tacit authority from Ministers to perform wrongful acts. We now add that the considerable time we have taken to examine the issues of approval or knowledge or toleration, express or implied, by government officials of wrongful acts by members of the R.C.M.P. has led us inevitably into the receipt of much testimony and the examination of many documents which relate to the relationship between government officials and the R.C.M.P. This testimony and these documents have been invaluable to us in giving us a comprehension of that relationship as a formulation for our recommendations under paragraph (c). As we, in this Report, summarize this evidence as a preliminary to making recommendations as to the future relationship between the government and the R.C.M.P. or between the government and the security intelligence agency, it will be difficult to avoid using language which may appear to some readers as an expression of opinion about the quality of the conduct of a Minister or his competence. Because of this, we think that it is important that we say something about our interpretation of our terms of reference as they may relate to the review of political judgment or the quality of decisions made by Ministers of the Crown.

46. We have had no hesitation in considering ourselves entitled to inquire into, and report on, any implication on the part of such persons in specific acts "not authorized or provided for by law" in which members of the R.C.M.P. are involved, or any implication on the part of such persons in wrongdoing generally by members of the R.C.M.P. This would include complicity or knowledgeable acceptance before the event, and also knowledge after the event. Moreover, we have inquired into, and will report on, the extent to which such

persons knew of the existence of any policies or practices of the R.C.M.P., the implementation of which would result in acts not authorized or provided for by law.

47. When the facts pass from the domain of issues of complicity in, or encouragement or tolerance or knowledge of, wrongdoing, to that of the quality of the conduct of a Minister or public servant in a general sense, we consider that we should be very cautious. While, in so far as the R.C.M.P.'s duties in connection with the protection of the security of Canada are concerned, paragraph (c) permits us to inquire broadly into laws, policies and procedures that affect the exercise of those duties, we draw a distinction between (i) inquiring into past and present laws, policies and procedures and reporting upon them as matters of fact, and (ii) passing judgment on the correctness of the decisions, or sometimes the lack of decision, that have led to the existence or absence of a law or a policy or a procedure. We have tried to avoid the latter as much as possible, for we do not consider that we are empowered to pass judgment on the quality of a Minister's "management". Yet we emphasize that our caution does not apply so as to cause us to refrain from comment if a Minister has been involved in illegality — whether by active participation before or after the event, knowledge of illegal activity combined with a failure to stop it or deal with it in some other proper way, or wilful blindness.

48. One of us is a judge, but what Dean G.E. Le Dain (now Mr. Justice Le Dain), chairman of the Commission Into the Non-Medical Use of Drugs, has written of judges is true also of Commissioners of Inquiry who are not judges:

> ... their experience is limited when it comes to passing judgment on political conduct. For one thing, a judge has no particular qualifications for the task, and secondly, the proper forum for the trial of such an issue is Parliament, and ultimately appeal to the electorate.[12]

As he points out, there have been instances in Canada when the terms of reference of a Commission of Inquiry appointed under Part I of the Inquiries Act have been broad enough that the Commission has had a duty not only to report facts but in effect to pass judgment on a Minister. However, the lesson we draw from his invaluable review of those instances is that it is only when the terms of reference clearly impose a duty to make comments or express opinions on the quality of the acts of Ministers or public servants (apart from wrongdoing) that a Commission of Inquiry should do so. As far as a judge who is a Commissioner is concerned, only adoption of such a view can minimize the danger where, in Dean LeDain's words, "serious political issues" are involved and "the life of the government itself may even be at stake". The confidence that is generally reposed by the public in the independence of the judiciary may be compromised if a Commissioner who is a judge does not avoid comment on such matters unless comment is required by his terms of reference.[13] On the other hand, it would be unrealistic to expect that a clear line can be drawn

---

[12] Gerald E. Le Dain (now the Honourable Mr. Justice Le Dain), "The Role of the Public Inquiry in our Constitutional System", in J.S. Ziegel (ed.), *Law and Social Change*, Toronto, Osgoode Hall Law School, York University, 1973, p. 86.

[13] *Ibid.*, p. 91.

between finding the facts about ministerial conduct or that of public servants and expressing an opinion or judgment about those facts. Despite efforts to clarify the distinction, findings of fact may sound like the expression of judgment about those facts. Moreover, the very use of judges in any inquiry which has any political implications inevitably produces what Professor John Willis, commenting on Dean LeDain's remarks, has called "an uneasy see-saw between the two irresistible desires" — one being "a desire to keep the judges' hands-off policy and the judges themselves out of politics", the other "a desire to give to the citizen the only decision-maker that he, whether rightly or wrongly, regards as truly independent and truly impartial, viz., a judge".[14]

The rights of individuals

49. In a statement made at a hearing on July 11, 1979 (Appendix G), we referred to a number of the policy and legal issues concerning which we intended to make recommendations pursuant to paragraph (c). As to these issues we observed that in considering them we were concerned with "both the consonance of Security Service activities with democratic values, and the effectiveness of the Security Service". Order-in-Council P.C. 1966-2148, which appointed the members of the Royal Commission on Security, expressly directed those Commissioners to have "regard to the necessity of maintaining (a) the security of Canada as a nation; and (b) the rights and responsibilities of individual persons" when they advised "what security methods and procedures are most effective". The point of our remark was to provide reassurance that, even though our Order-in-Council does not refer to the rights of individuals, we intended from the outset to place them on the scales as we weighed the policy and legal recommendations we might make. We have endeavoured, in this Report, to honour that commitment.

Our access to documents

50. A great deal of testimony received by us, particularly since October 1978, has been testimony of past and present Ministers of the Crown and public servants. In preparation for their testimony, and for that of past Commissioners of the R.C.M.P. and the previous Director General of the Security Service, and of the present Commissioner and Director General, we have obtained many documents that have been in the possession of departments of the government or that originated with them but were found by us in the possession of the R.C.M.P. There has been no difficulty in obtaining most such documents, except that, after the administration of the Right Honourable Joe Clark took office on June 5, 1979, the process of obtaining documents originating during the period when the Right Honourable Pierre Elliott Trudeau was Prime Minister, was complicated by the need to comply with Order-in-Council P.C. 1979-1616, dated June 2, 1979 (Appendix K). Even before that, however, there were two important developments in regard to government documents. One was our statement of October 13, 1978, in which we said that the decision as to whether documents might not be produced in public on the grounds of

[14] Professor Willis was commenting on Dean Le Dain's paper. His comments are found in the same volume, at p. 100.

national security was for us to make and not the Solicitor General, and that, similarly, the power to decide whether documents such as Cabinet Ministers' memoranda to Cabinet and letters between Ministers should be disclosed publicly rested with ourselves rather than the Privy Council. In reaching the latter decision, we itemized a number of considerations which we might properly take into account in deciding particular cases. We expressed optimism that in particular cases in the future the Commissioners and counsel for all parties (including the government) would be able to arrive at a mutually satisfactory result. We are happy to say that so far, one way or another, that has been possible. The second development that we should note was that, in order to facilitate our inquiry into possible implication of Ministers in acts not authorized or provided for by law, the government adopted Order-in-Council P.C. 1979-887, dated March 22, 1979 (Appendix J). It provided a detailed procedure to govern our access to a particular class of government documents, namely, the minutes of any Cabinet or Cabinet Committee meeting. It allowed us access to the minutes of any such meeting "held prior to the establishment of the Commission which relate to the terms of reference of the Commission... and which on reasonable and probable grounds [we] believe provide evidence establishing the commission of any act involving members of the R.C.M.P. or persons who were members of the R.C.M.P. that was not authorized or provided for by law, or evidence implicating a Minister in such act". We took advantage of this provision and shall report on the result in a subsequent Report.

THE WORK OF THE COMMISSION

A. ORGANIZATION

51. As pointed out earlier in this part of our Report, the terms of reference of this Commission are unusual in that they require not only the examination of specific acts, but also a general review and reporting on policies, procedures and laws. To fulfill this dual role it has been necessary to create two sections in the Commission, one engaged in legal matters ranging from investigations to hearings to legal arguments, and the other doing research into policy issues with and without legal ramifications. Clearly there had to be close cooperation between the two groups, but their functions were distinct in many regards. To keep duplication to a minimum, common administrative services were developed. As preparation of this Report progressed, the work of the two sections gradually merged to ensure a comprehensive whole.

B. PERSONNEL

52. Our initial concern was to recruit a Secretary, Chief Counsel, and Director of Research. Because of the magnitude of the task assigned, both at the outset and as it unfolded almost daily during the weeks following our appointment, it took some time to recruit persons with the qualifications necessary for those positions. In consultation with them we recruited the rest of the staff as the need arose. Because of the nature of the issues, we sought to obtain legal and research personnel who were previously unassociated with the Government of Canada or the R.C.M.P. We needed a team of trained investigators because of the numerous allegations made with respect to the activities of the R.C.M.P. and our mandate to investigate them. These investigators had to be independent and objective, to gain the confidence of the public, and also competent and fair, to win the confidence of the R.C.M.P. To that end, from within the federal government we obtained two investigators from the Department of National Defence, one from the National Harbours Board Police, and four officers of the Ontario Provincial Police.

53. Appendix L to this report is a list of the personnel who have worked for the Commission for varying periods of time.

C. WORK AND ACTIVITIES

54. The work and activities of the Commission can conveniently be broken down into several categories: investigations, hearings, formal briefings, informal meetings, visits to other countries, and research.

Investigations

55. In October 1977, we advertised in most of the daily newspapers and a number of the ethnic newspapers across Canada, inviting the public to submit to us any allegations they wished to make regarding conduct which fell within parts (a) and (b) of our terms of reference, and also any opinions they wished to express with respect to part (c) of those terms of reference (Appendix M). In October 1979, we advised the public, through advertisements in the daily newspapers, that no allegations would be investigated by us if received subsequent to November 19, 1979 (Appendix N). Over the course of our work we have received from individuals and organizations 292 allegations which *prima facie* fell within our mandate and 124 written submissions with respect to policies, procedures and laws. In addition, a number of allegations were brought to our attention indirectly through the news media. All allegations have been investigated, or are still in the process of being investigated, by us. A full examination of what we have done in this regard will be contained in a subsequent Report.

Hearings

56. The hearings have been of two kinds, those to receive evidence and those to receive presentations of briefs. The evidentiary hearings were both in public and *in camera*. Since October 18, 1977, the date of our first hearing, we have held 169 public hearings and 144 *in camera* hearings at which we have examined 149 witnesses (Appendix O) and have received 805 exhibits. A great deal of the *in camera* testimony was later made public. The evidentiary hearings have dealt with a number of major topics, which for brevity are described as follows:

- Operation Bricole — the A.P.L.Q. Incident
- Operation Ham — the removal and copying of Parti Québecois tapes
- Surreptitious Entries (generally)
- Certain cases of attempted recruitment of Human Sources
- Mail Checks
- Burning of a Barn
- Removal of Dynamite
- Access to information in the possession of the Department of National Revenue, the Unemployment Insurance Commission and other government departments
- Operation Checkmate — countermeasures and disruptive tactics
- Miscellaneous topics relating to the accountability of the R.C.M.P. to Government
- The Relationship between the Security Service and its Human Sources

Evidence was received on those topics first as to the activities which took place at the field level and then with respect to the knowledge and responsibility of senior officials and Ministers. We heard evidence of the extent to which those senior officials and Ministers had knowledge of either specific acts or general practices which it was our responsibility to investigate.

57. It was our view from the outset that as much as possible of the evidence relating to "acts not authorized or provided for by law" should be made public. This was subject, of course, to the restrictions imposed upon us by our mandate as to matters related to "national security", "public interest" or "the interest of the privacy of individuals". Most of the evidence was heard in public. Evidence that was heard initially *in camera* was reviewed by us and, after receiving representations from all interested parties, was expurgated by us as was considered necessary in the light of the restrictions mentioned, and released publicly. Evidence was received publicly on 142 days, each one represented by a volume of transcript. In addition, 52 volumes of transcript originally heard *in camera* have been edited and released in 45 volumes. During the course of the hearings we have been called upon to render a number of decisions with respect to both procedural and substantive questions. Copies of the reasons for a number of the major decisions are also annexed (Appendices E, F, G, H, I, and Z). Most of the witnesses who appeared before us have been represented by counsel. In Appendix P, we have set out the various counsel who have so appeared and the clients whom they represented.

58. The hearings to receive public briefs were held in Vancouver (twice), Regina, Toronto, Montreal, Fredericton and Ottawa (five times). The places and dates of such hearings and the names of the persons appearing at them are found in Appendix Q. We had also scheduled such hearings for Victoria, Calgary, Edmonton, Winnipeg, Halifax, Charlottetown and St. John's, and additional hearings in Toronto and Montreal. In spite of considerable advertising in the printed media, the response from the public was less than we had expected and we therefore consolidated the hearings regionally in the cities previously noted. When a hearing in any centre was cancelled the Commission paid the travelling expenses to another centre of all persons wishing to present submissions.

Formal briefings

59. The purpose of these briefings was to help us to inform ourselves as to both facts and opinions on matters which could not in any way be characterized as "misconduct" on the part of any person. The briefings were to assist us in carrying out our responsibilities under part (c) of the terms of reference. Before commencing hearings and setting up our research programme, we met with officials of a number of departments which have some security role in the government. In this way we could familiarize ourselves with the extent of the federal government involvement in security and the relationships those departments with security roles have with the Security Service of the R.C.M.P. Since those initial briefings, we have had, during the course of the work of the Commission, numerous others from the R.C.M.P. and government departments covering, in great detail, all aspects of the role played by the R.C.M.P. and those departments in security matters. A list of the topics on which we have had briefings is found in Appendix R.

Informal meetings

60. To supplement the information that we obtained at the hearings and the formal briefings, we met informally with a number of groups and individuals to

obtain their opinions on various topics relating to the policies, procedures and laws which ought to apply to security matters.

61. We began this process of informal consultation by bringing together groups of academics on two separate occasions: November 25 and 26, 1977, in Toronto, and February 24 and 25, 1978, in Montreal. The Toronto meeting was conducted in English and the Montreal meeting in French. Those attending are listed in Appendix S. We wished to obtain from these academics and scholars guidance as to the direction which our research programme ought to take, and some general ideas as to how we ought to implement that programme. The meetings accomplished both of those purposes as well as providing us with some useful contacts for carrying out the programme.

62. In January 1979, in Regina, we held a seminar to which we invited representatives of those sectors of society whose lives might be more directly affected by the activities of the Security Service or who for some other reason had a particular interest in the subject.

63. In addition to a number of visits which we made to R.C.M.P. Headquarters in Ottawa for specific purposes, one or more of us toured Security Service offices in Montreal, Toronto, Ottawa, Vancouver and Edmonton where we spent some time discussing with members at all levels their job functions and problems they might be experiencing. This gave us a sense of the organization that we would not otherwise have had. We attempted to get some feeling for the role played by the recruit training programme at Regina in shaping future regular members and more particularly members assigned to the Security Service. To that end we visited the Regina depot observing classes in progress and discussing with the teaching staff the curriculum, the recruits' lifestyle during training and what the training is designed to accomplish.

64. In a further attempt to identify problems that might be facing the Force, and particularly the Security Service, in the different regions, we met with divisional Commanding Officers and Heads of the Security Service in British Columbia, Saskatchewan, Southwestern Ontario, Ontario, Quebec and New Brunswick. We also attended a Commanding Officers' Conference in Ottawa where we had a round table discussion with the Commanding Officers and senior officers from Headquarters.

Foreign study and visits

65. It became apparent to us early in our mandate that the nature of the problems we had been asked to examine was not unique to Canada. We also became aware that a number of reviews such as that which we had been commissioned to undertake had been carried out in other countries with similar backgrounds to our own. To obtain a clear picture of the current situations in the U.S.A., the United Kingdom, Australia and New Zealand, we asked leading academics in the security field in each of those countries to provide us with a comprehensive report based on publicly available material. The authors of those studies are included in Appendix T. Having obtained those composite studies and after talking to a number of officials at the most senior levels in the Canadian government security community, we realized that there are very few

people with a broad perception of the problems, or who have given any serious and informed consideration to their resolution. To assist us in our task we therefore visited those four countries (U.S.A., United Kingdom, New Zealand and Australia) where we had discussions with past and present politicians and senior officials who have played a major role in police and security matters. It was a condition of the consent of each of those countries to these discussions that our visits be kept confidential. We have therefore not included here a list of the persons with whom we met. Details of the meetings are to be found in our Commission records. We would not, however, be breaching any confidence by disclosing that we met with Mr. Justice R.M. Hope of Australia and Sir Guy Powles of New Zealand, both in Canada and in their respective homelands. Each of those gentlemen has conducted an examination similar to ours for his own country.

66. In addition we instructed our Director of Research and Secretary to visit the Netherlands and the Federal Republic of Germany, and the Director of Research and one of our counsel to visit France, to determine whether there were any aspects of policing and security in those countries which were sufficiently similar to our own that we could benefit from a visit to them. The reports which we received after those visits disclosed some very helpful information but we determined that a visit by us would not be of sufficient further benefit having regard to the necessary rationing of our time. In reaching this decision we took into account that of those countries we did visit, the United Kingdom, New Zealand, and Australia have constitutional systems most similar to our own, and the United States, while it has a different Constitution, has undertaken serious examination of its intelligence community in recent years.

Research studies

67. Our research and legal staffs have done extensive background studies for us covering many facets of our work. However, during the course of the Commission some matters have required such a major study or such a special expertise that they had to be carried out by researchers outside the Commission. Including the four studies by foreign academics previously mentioned, 21 such research papers have been written for us. Also, in certain areas of research we felt that we needed assistance from experts. We therefore retained consultants to help us. The titles of the papers and the authors and the names of the consultants and the areas of consultation are set out in Appendix T. Three of the major studies have been published by the Government of Canada at our request and are available to the public through the usual distribution channels for government publications. Those studies are:

1. *Parliament and National Security*, by Prof. C.E.S. Franks of Queen's University.
2. *Ministerial Responsibility for National Security*, by Prof. J.Ll. J. Edwards of the University of Toronto.
3. *National Security : The Legal Dimensions*, by Prof. M.L. Friedland of the University of Toronto.

We sought the publication of those studies in the hope of obtaining public response to the views taken by the authors. We hoped in that way to obtain some fresh insights into the problems. We also hoped that such additions to the sparse background material relating particularly to Canada might assist in any future consideration of the problems and might also generate future studies.

Meetings with Ministers, Members of Parliament and Senior Officials

68. As we began to clarify the problems facing us and to formulate tentative solutions, we considered it advisable to discuss the problems with those people in government who might have further information or opinions, or who might be required to play a role in implementing our recommendations. Consequently, we undertook a series of meetings with past and present Ministers of the Crown, Members of Parliament, and senior officials at both the federal and provincial level. Thus, we met privately with the following past and present Solicitors General:

Hon. Jean-Pierre Goyer
Hon. W.W. Allmand
Hon. Francis Fox
Hon. Jean-Jacques Blais
Hon. Allan Lawrence
Hon. Robert Kaplan,

the following past and present party leaders:

Rt. Hon. J.G. Diefenbaker
Rt. Hon. J. Clark
Hon. R.L. Stanfield
Mr. T.C. Douglas
Mr. E. Broadbent,

and the following past and present Members of Parliament:

Hon. Mark MacGuigan
Hon. Wm. Jarvis
Hon. Elmer MacKay
Mr. G.W. Baldwin
Mr. G.W. Fairweather,

The past and present senior officials of both the government of Canada and some provincial governments with whom we have met privately are set out in Appendix W. Of course, in addition to those persons mentioned above with whom we met personally, our researchers have had numerous interviews with government officials at all levels to obtain information and assistance in preparing reports for us.

D. LAW SUITS

69. Two separate law suits have been brought against us in the Federal Court of Canada. The first was launched by Paul D. Copeland on his own behalf and on behalf of all members of the Law Union of Ontario. It was an application

for a writ of prohibition having the effect of preventing us from continuing our inquiry. The application was dismissed on August 4, 1978. The judgment and reasons for decision of Mr. Justice Cattanach, are found in Appendix X. The second suit was brought against us by Ross Dowson and John Riddell. This application was for a writ of certiorari with mandamus in aid to quash our decision refusing Messrs. Dowson and Riddell the right to examine witnesses before us and requiring us to grant the applicants such right. That application was dismissed by Mr. Justice Gibson on June 2, 1980. A copy of the Order of dismissal is found in Appendix Y.

BIOGRAPHICAL REFERENCE

Ministers, senior officials and senior R.C.M.P. officers who figure in this Report

In alphabetical order:

ALLMAND, The Hon. Warren W.: Solicitor General, November 27, 1972, to September 14, 1976.

BARRETTE, J.E.M.: Assistant Commissioner of R.C.M.P. (ret.). Assistant Director of R.C.M.P. Security and Intelligence, August 29, 1967, to August 8, 1969; Director of R.C.M.P. Security and Intelligence, August 9, 1969, to December 31, 1969.

BISSONNETTE, P.A.: Deputy Solicitor General, November 28, 1977, to present.

BLAIS, The Hon. Jean-Jacques: Solicitor General, February 2, 1978, to June 4, 1978.

BOURNE, Robert (Robin) Colonel (ret.): Head, SPARG (Security Planning and Research Group now known as Police and Security Branch), June 1, 1971, to June 1, 1979. In July 1972, he was also made Assistant Deputy Solicitor General.

CLARK, The Rt. Hon. Joe: Prime Minister and Chairman of the Cabinet Committee on Security and Intelligence, June 5, 1979, to March 4, 1980.

COTE, Ernest A.: Deputy Solicitor General, December 14, 1968, to July 31, 1972.

DARE, Michael R. Lt. General (ret.): Director General, R.C.M.P. Security Service, May 1, 1973, to present.

DRAPER, Howard C.: Assistant Director of R.C.M.P. Security and Intelligence, September 8, 1969, to August 17, 1971; Assistant Deputy Director General (Operations), R.C.M.P. Security Service, August 17, 1971, to September 1, 1972; Deputy Director General (Operations), R.C.M.P. Security Service, September 1, 1972, to July 31, 1975.

FOX, The Hon. Francis: Solicitor General, September 14, 1976, to January 28, 1978.

GIROUX, J.E.J.B.: Assistant Commissioner of the R.C.M.P.; Deputy Director General (Operations), R.C.M.P. Security Service, January 3, 1978, to present.

GOYER, The Hon. Jean-Pierre: Solicitor General, December 22, 1970, to November 27, 1972.

HIGGITT, W. Leonard: Assistant Director of R.C.M.P. Security and Intelligence, October 19, 1964, to July 31, 1967; Director of R.C.M.P. Security and Intelligence, August 1, 1967, to September 7, 1969; Commissioner of the R.C.M.P., October 1, 1969, to December 31, 1973.

KAPLAN, The Hon. Robert P.: Solicitor General, March 4, 1980, to present.

KELLY, William H.: Deputy Commissioner of the R.C.M.P. (ret.). Director of R.C.M.P. Security and Intelligence, October 19, 1964, to August 10, 1967.

LAWRENCE, The Hon. Allan F.: Solicitor General, June 4, 1979, to March 4, 1980.

LINDSAY, M.F.A.: Commissioner of the R.C.M.P., August 15, 1967, to September 30, 1969.

MASSE, Marcel: Clerk of the Privy Council and Secretary to the Cabinet, June 1979 to March 1980; Chairman of the Interdepartmental Committee on Security and Intelligence, June 1979 to March 1980.

MacDONALD, T.D.: Deputy Solicitor General, October 1, 1966, to December 13, 1968.

McCLELLAN, George B.: Commissioner of the R.C.M.P., November 1, 1963, to August 14, 1967.

McILRAITH, The Hon. George J.: Solicitor General, July 6, 1968, to December 22, 1970.

NADON, Maurice: Commissioner of the R.C.M.P., January 1, 1974, to August 31, 1977.

PEARSON, The Rt. Hon. Lester B.: Prime Minister and Chairman of the Cabinet Committee on Security and Intelligence, April 22, 1963, to April 20, 1968.

PENNELL, The Hon. Lawrence: Solicitor General, July 7, 1965, to April 20, 1968.

PITFIELD, P. Michael: Clerk of the Privy Council and Secretary to the Cabinet, January 1972 to June 1979, and March 1980 to present; Chairman of the Interdepartmental Committee on Security and Intelligence, December 1977, to June 1979 and March 1980, to present.

ROBERTSON, R.G.: Clerk of the Privy Council and Secretary to the Cabinet, and Chairman of the Security Panel, July 1963, to January 1972; Chairman of the Interdepartmental Committee on Security and Intelligence, January 1972, to December 1977.

SEXSMITH, Murray: Assistant Commissioner; Deputy Director General (Operations), R.C.M.P. Security Service, July 16, 1975, to January 28, 1978.

SIMMONDS, Robert H.: Commissioner of the R.C.M.P., September 1, 1977, to present.

STARNES, John: Director General, R.C.M.P. Security Service, January 1, 1970, to April 30, 1973.

TASSE, Roger: Deputy Solicitor General, August 1, 1972, to November 27, 1977; Deputy Minister of Justice, November 27, 1977, to present.

TRUDEAU, The Rt. Hon. Pierre E.: Prime Minister and Chairman of the Cabinet Committee on Security and Intelligence, April 20, 1968, to June 5, 1979 and March 4, 1980, to present.

TURNER, The Hon. John N.: Solicitor General, April 20, 1968, to July 6, 1968.

By position:

Prime Ministers

April 22, 1963, to April 20, 1968.	The Rt. Hon. Lester B. Pearson.
April 20, 1968, to June 5, 1979.	The Rt. Hon. Pierre E. Trudeau.
June 5, 1979, to March 4, 1980.	The Rt. Hon. Joe Clark.
March 4, 1980, to present.	The Rt. Hon. Pierre E. Trudeau.

Chairmen — Cabinet Committee on Security and Intelligence

April 22, 1963, to April 20, 1968.	The Rt. Hon. Lester B. Pearson.
April 20, 1968, to June 5, 1979.	Rt. Hon. Pierre E. Trudeau.
June 5, 1979, to March 4, 1980.	The Rt. Hon. Joe Clark.
March 4, 1980, to present.	The Rt. Hon. Pierre E. Trudeau.

Solicitors General

July 7, 1965, to April 20, 1968.	The Hon. Lawrence Pennell.
April 20, 1968, to July 6, 1968.	The Hon. John N. Turner.
July 6, 1968, to December 22, 1970.	The Hon. George J. McIlraith.
December 22, 1970, to November 27, 1972.	The Hon. Jean-Pierre Goyer.
November 27, 1972, to September 14, 1976.	The Hon. Warren W. Allmand.
September 14, 1976, to January 28, 1978.	The Hon. Francis Fox.
February 2, 1978, to June 4, 1978.	The Hon. Jean-Jacques Blais.
June 4, 1979, to March 4, 1980.	The Hon. Allan F. Lawrence.
March 4, 1980, to present.	The Hon. Robert P. Kaplan.

Chairman — Security Panel
(existed only until 1972)

July 1963, to January 1972.	Mr. R.G. Robertson.

Chairmen — Interdepartmental Committee on Security and Intelligence (formed 1972)

January 1972, to December 1977.	Mr. R.G. Robertson.
December 1977, to June 1979.	Mr. P.M. Pitfield.
June 1979, to March 1980.	Mr. Marcel Massé.
March 1980, to present.	Mr. P.M. Pitfield.

Deputy Solicitors General

October 1, 1966, to December 13, 1968.	Mr. T.D. MacDonald.
December 14, 1968, to July 31, 1972.	Mr. Ernest A. Côté.
August 1, 1972, to November 27, 1977.	Mr. Roger Tassé.
November 28, 1977, to present.	Mr. P.A. Bissonnette.

Heads — Security Planning and Research Group
(now known as Police and Security Branch,
Department of the Solicitor General)

June 1, 1971, to June 1, 1979.	Colonel (ret.) Robert (Robin) Bourne.
June 1, 1979, to present.	Mr. Michael Shoemaker.

Commissioners of the R.C.M.P.

November 1, 1963, to August 14, 1967.	Mr. George B. McClellan.
August 15, 1967, to September 30, 1969.	Mr. M.F.A. Lindsay.
October 1, 1969, to December 31, 1973.	Mr. W. Leonard Higgitt.
January 1, 1974, to August 31, 1977.	Mr. Maurice Nadon.
September 1, 1977, to present.	Mr. Robert H. Simmonds.

Directors of R.C.M.P. Security and Intelligence
(1964-69)

October 19, 1964, to August 10, 1967.	Mr. William H. Kelly.
August 1, 1967, to September 7, 1969.	Mr. W. Leonard Higgitt.
August 9, 1969, to December 31, 1969.	Mr. J.E.M. Barrette.

Directors General of the R.C.M.P. Security Service
(1970 to present)

January 1, 1970, to April 30, 1973.	Mr. John Starnes.
May 1, 1973, to present.	Mr. Michael R. Dare.

Assistant Directors of R.C.M.P. Security and Intelligence
(1964-71)

October 19, 1964, to July 31, 1967.	Mr. W. Leonard Higgitt.
August 29, 1967, to August 8, 1969.	Mr. J.E.M. Barrette.
September 8, 1969, to August 17, 1971.	Mr. Howard C. Draper.

Assistant Deputy Directors General (Operations)
of R.C.M.P. Security and Intelligence
(1971-72)

August 17, 1971, to September 1, 1972.	Mr. Howard C. Draper.

Deputy Directors General (Operations)
of R.C.M.P. Security Service
(1972-)

September 1, 1972, to July 31, 1975.	Mr. Howard C. Draper.
July 16, 1975, to January 28, 1978.	Mr. Murray S. Sexsmith.
January 3, 1978, to present.	Mr. J.E.J.B. Giroux.

PART II

THE SECURITY SYSTEM: THE NATURE OF GOVERNMENTAL CONCERN AND INVOLVEMENT

CHAPTER 1: Security and Democracy: Interests Requiring Protection and Threats to Those Interests

CHAPTER 2: The Organizational Response by Government

INTRODUCTION

1. In this part of our Report we provide an account of the basic elements of Canada's security system, its underlying purpose and principles, and the structures which have been put in place to provide security and intelligence. The focus here is on the Security Service of the R.C.M.P. In Part III, which deals with what might be called a breakdown in the system, we report on R.C.M.P. practices and activities "not authorized or provided for by law" on both the criminal investigation side of the Force and on the Security Service side. This is, of course, in conformity with the Commission's terms of reference which instruct it to report on the extent and prevalence of such activities and practices on both sides of the R.C.M.P. but require a *comprehensive* review of policies, procedures and laws only with respect to the security responsibilities of the Force.

CHAPTER 1

SECURITY AND DEMOCRACY: INTERESTS REQUIRING PROTECTION AND THREATS TO THOSE INTERESTS

A. THE NEED FOR SECURITY

2. Paragraph (c) of our terms of reference calls upon us to report and make recommendations on the policies, procedures and laws governing the activities of the R.C.M.P. in the discharge of its responsibility to protect "the security of Canada". The terms of reference do not explain what is meant by the phrase "the security of Canada", and yet some explanation is surely required. In recent years in our own country and other Western democracies, we have experienced the dangers of using such a term too loosely. All manner of questionable activities encroaching on civil liberties may be perpetrated on the citizens and residents of a country in the name of national security. In response to this experience there has been a tendency in some quarters to reject the concept of 'national security' entirely and to rely instead on concepts that are more readily understood, such as 'national defence' and 'law enforcement'. But we question whether these alternative phrases adequately cover the security activities that, in our view, need to be carried out in all states, including Canada.

3. The Royal Commission on Security which reported in 1968 on the operation of Canadian security methods and procedures gave its understanding of the meaning of the "security of Canada". In its view, it was the indisputable duty of the state

> . . . to protect its secrets from espionage, its information from unauthorized disclosure, its institutions from subversion and its policies from clandestine influence.[1]

In our First Report on *Security and Information*, without attempting to be exhaustive, we stated that, in our opinion, there were two concepts involved in the "security of Canada":

> The first is the need to preserve the territory of our country from attack. The second concept is the need to preserve and maintain the democratic

[1] *Report of the Royal Commission on Security*, Ottawa, 1969, paragraph 28.

processes of government. Any attempt to subvert those processes by violent means is a threat to the security of Canada.[2]

Fundamental to both these definitions are two basic needs: first, the need to protect Canadians and their governments against attempts by foreign powers to use coercive or clandestine means to advance their own interests in Canada, and second, the need to protect the essential elements of Canadian democracy against attempts to destroy or subvert them. These, we believe, are fundamental security requirements which must be met in Canada if our country is to be truly self-governing.

4. The threats to Canada's security against which protection is needed today and in the foreseeable future fall into three basic categories: activities of foreign intelligence agencies, political terrorism, and subversion of democratic institutions. We will be expanding on these three threats throughout this Report and will make only a few germane comments about them here.

5. First, there are the clandestine activities of agents of foreign powers in Canada. These have not lessened, although Canada has not been at war for many years and a relaxation of international tensions has been associated with what is perhaps somewhat optimistically referred to as East-West détente. On the contrary, in recent years, the number of foreign intelligence agencies has increased, as have the attempts to use these agencies against Canada, both to obtain intelligence and to influence Canadian policies.

6. A second type of threat to Canadian security arises from politically motivated acts of violence and threats of violence aimed at forcing governments to act in a certain way. Today, the popular word for activities of this kind is 'terrorism'. The internationalization of terrorist activities since the late 1960s has significantly increased the severity of this threat to the security of Canada. (It is interesting to note that the 'terrorist' threat to security was not even mentioned in the Report of the Royal Commission on Security, which reported in 1968.) It would be rash to predict a disappearance of the 'terrorist' threat in the future: political fanaticism is not on the wane, and modern technology increases the power of a few to threaten the many. Protection against terrorism is likely to be a security requirement for many years to come.

7. The third category of threat to Canada's security today and in the future concerns activities of those whose objectives are to subvert or destroy the democratic system of government in Canada. Fortunately, since the Second World War subversive organizations on the extreme left and the extreme right of the political spectrum have not posed a serious threat to the democratic process in Canada. There remain, however, a few small groups, some with considerable foreign support, which are committed to the destruction of democracy in Canada. A democratic state such as Canada has a duty to protect itself against those who work actively to overthrow the foundations of our parliamentary democracy: namely, free elections with universal adult

[2] *Security and Information, First Report of the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police*, Ottawa, 1979, paragraph 38.

suffrage, free public discussion about public affairs, freedom of the press, freedom of assembly for the purpose of organizing and marshalling public opinion about political matters, and the application of the rule of law.

8. One way in which Canada's internal security is protected is through the enforcement of the criminal law. Law enforcement agencies at the federal, provincial and municipal levels have an important role to play in apprehending those who conspire or attempt to carry out, or who have carried out, an act of espionage, terrorism or subversion against the democratic system. But the security of Canada would be badly served if this were the only form of protection. Advance intelligence is needed to prevent espionage networks or terrorist support systems being established in Canada. Government departments need reliable information on which to judge whether persons being considered for positions involving access to secret information are security risks. Immigration and Citizenship officials similarly require reliable information as to whether persons applying for entry to Canada or for Canadian citizenship are participants in activities endangering the security of Canada. Those responsible at the federal and provincial levels for securing strategic installations, such as nuclear power stations or defence production centres, from sabotage or espionage need advice on the nature of possible attacks and on appropriate protective measures. Similarly, the security of international events in Canada, such as the Olympic Games, the Habitat Conference and the Commonwealth Games, and of visiting international dignitaries and our own political and governmental leaders, requires timely advance assessments of the source and techniques of possible terrorist attacks.

9. In a word, a democratic state needs security intelligence to protect itself against attack on its democratic values and procedures. That is why all of Canada's democratic allies have developed organizations, either within or alongside their police forces, which specialize in security intelligence work, collecting and reporting intelligence about threats to internal security to appropriate government departments and law enforcement agencies. A security system thus requires the capacity to obtain and report timely intelligence to those executive agencies responsible for taking lawful protective measures against threats to security.

10. But in our mind there is more than just an internal need for a security intelligence agency. Canada's international alliances require that it be able to assure its allies, with whom it participates in common defence arrangements, that it has a sound system of internal security. Allied countries will not entrust Canadian officials and political leaders with secret information unless Canada has in place effective structures and procedures for detecting and preventing foreign espionage. Similarly, Canada is a signatory to a number of international agreements providing for cooperation in combatting terrorism.[3] These agreements provide Canada with international support in the event of a terrorist attack on Canadians at home or abroad, and they entail a correspond-

[3] L.C. Green, "Terrorism — The Canadian Perspective", in *International Terrorism: National, Regional and Global Perspectives*, ed. by Y. Alexander, New York, Praeger, 1976.

ing responsibility for Canada to assist other countries subjected to terrorist attacks.

11. The security of Canada, as we understand it, is a concern of both levels of government in Canada. Canada is a federal state: it is essential that the democratic character of government, both federal and provincial, be secured from clandestine foreign interference and attempts at violent subversion.

12. The British North America Act[4] does not explicitly assign legislative jurisdiction over security to either level of government. The federal Parliament's power to make laws for the peace, order and good government of Canada in relation to all matters not exclusively assigned to the provinces, undoubtedly provides constitutional support for a large federal role in security, especially in emergency situations. In the Alberta Press Act case in 1938, Chief Justice Duff of the Supreme Court of Canada held that

> ... the powers requisite for the protection of the constitution itself arise by necessary implication from the British North America Act as a whole...and since the subject matter in relation to which the power is exercised is not exclusively a provincial matter, it is necessarily vested in Parliament.[5]

Mr. Justice Fauteux of the Supreme Court, in the case of *Switzman* v. *Elbling* in 1957, stated that

> ... questions which are of the order of the security of the state cannot be considered a matter of a purely local or private character within the province.[6]

Further constitutional support for the federal government's role in safeguarding the security of Canada may be found in its exclusive jurisdiction over Defence and over Criminal Law and Criminal Procedure. Under the latter power the federal Parliament has identified the criminal offences which relate to security, for example, treason, seditious libel, seditious conspiracy, uttering seditious words, sabotage, and espionage.

13. However, the provinces too have security concerns and responsibilities. The provinces are concerned with securing provincial and municipal institutions against subversive attack. In exercising their responsibility for the appointment of provincial officials, provincial governments need information about persons who constitute security risks. The provinces' responsibility for the administration of justice gives them a primary role in taking police and prosecutorial measures against persons, such as terrorists, when their activities against Canadian security have escalated to the point of becoming criminal offences.

14. Whatever the constitutional niceties, it is clear that from a practical point of view both levels of government have important roles to play in meeting Canada's security requirements. Most of the activities threatening Canada's security have national and international dimensions. The federal government should have the primary responsibility for collecting intelligence about these

---

[4] (1867) 30 & 31 Vic., ch.3 (U.K.). Reproduced in R.S.C. 1970, Appendices.

[5] *Reference re: Alberta Statutes* [1938] S.C.R. 100, at pp. 133-134.

[6] *Switzman* v. *Elbling and Attorney General for Quebec* [1957] S.C.R. 285, at p. 324.

threats and for coordinating measures to protect Canadians and international visitors from them. Provincial and municipal authorities have a primary responsibility for the enforcement of law and maintaining peace at the local level. In security matters these respective responsibilities will frequently intersect. In relation to terrorism, for example, federal agencies should endeavour to obtain intelligence about the identity, movement and techniques of persons in Canada who are associated with international terrorist groups or who receive support for terrorist activities from foreign countries. This intelligence should be shared with provincial and municipal authorities to assist them in taking measures to protect foreign visitors and Canadian V.I.P.s within their jurisdictions, and to assist local police in apprehending persons participating in acts of political violence.

15. The effective provision of security in a federal state requires close cooperation among all levels of government. For this reason, we believe it would be a mistake to assume that the security requirements and functions we have identified above can be swept into a sphere of exclusive federal jurisdiction simply by attaching the label 'national security' to them. Safeguarding Canada from attempts by foreign-directed or purely domestic groups to subvert Canadian democracy will be jeopardized if 'national security' becomes a subject of federal-provincial rivalry. Later in this Report, when we turn to our proposals for a Security Plan for the Future, we shall make some recommendations about ways and means of improving federal-provincial cooperation with regard to the security of Canada.

B. SECURITY AND THE REQUIREMENTS OF LIBERAL DEMOCRACY

16. Liberal democracies face a unique challenge in maintaining the security of the state. Put very simply, that challenge is to secure democracy against both its internal and external enemies, without destroying democracy in the process. Authoritarian and totalitarian states do not have to face this challenge. In such countries there is no need to ensure that security agencies, whose techniques inevitably involve a great deal of secrecy, be accountable to an elected legislature. Nor is there a requirement in such states that all of their security measures be authorized or provided for by law and that none of their officials be above the law. Only liberal democratic states are expected to make sure that the investigation of subversive activity does not interfere with the freedoms of political dissent and association which are essential ingredients of a free society.

17. Canada must meet both the requirements of security and the requirements of democracy: we must never forget that the fundamental purpose of the former is to secure the latter. Those who seek to subvert Canada's democratic institutions would realize an ironic victory if Canadians were to permit their governors to violate the requisites of democracy in the course of protecting them from its opponents.

18. Providing effective security within a liberal democracy has in recent years come to be acknowledged as a major problem of public policy in most Western

democracies. That challenge, which is at the centre of our work, has been the underlying purpose of inquiries into the activities of security and intelligence agencies in Australia, New Zealand, the United Kingdom and the United States. In Australia, Mr. Justice Hope was appointed in 1974 as a single Commissioner to carry out a comprehensive study of Australia's security system. His reports, submitted in 1977, led to the enactment in 1979 of a new charter for the Australian Security Intelligence Organization. In 1976, Sir Guy Powles, the Chief Ombudsman of New Zealand, completed a study of the practices, procedures and organization of that country's security intelligence agency. In the United Kingdom there has been a series of special studies and reports on security problems going back to the 1955 Privy Councillors' Report on Security, and including the Radcliffe Report in 1962 on Security Procedures in the Public Service and Lord Denning's Report on the Profumo affair in 1963. In March 1980, the Secretary of State for the Home Department (the Home Secretary) submitted a report to Parliament on the interception of communications in relation to security and criminal investigations. In the United States, a Commission chaired by Vice-President Rockefeller reported in 1975 on C.I.A. activities within the United States. A year later, a Select Committee of the United States Senate, chaired by Senator Church, completed a six-volume report on the intelligence activities of the United States. The Church Report provided the foundation for the drafting of proposed comprehensive legislative charters for intelligence agencies in that country. The opening page of the Rockefeller Report sets out the following statement (which quotes, in part, President Ford's announcement of the establishment of the Commission) of the challenge which confronts all democracies with regard to their security arrangements:

> While it is vital that security requirements be met... it is equally important that intelligence activities be conducted without impairing our democratic institutions and fundamental freedoms.[7]

19. In taking the position that the requirements of security in Canada must be reconciled with the requirements of democracy, let us be clear that we regard responsible government, the rule of law, and the right to dissent as among the essential requirements of our system of democracy.

20. By responsible government we mean that there must be effective procedures for ensuring that those who carry out security investigations and other security measures are accountable to Ministers of the Crown, who in turn are responsible to Parliament. Security activities of necessity involve a great deal of secrecy because they are normally being carried out to detect and prevent secret activities. Security operations, to be effective, cannot be an open book to the whole world, but it does not follow that they cannot be an open book to responsible Ministers. The Honourable Robert Stanfield, then Leader of the Opposition, put this point very well in 1969 when he said in the House of Commons:

---

[7] *Report to the President by the Commission on C.I.A. Activities within the United States*, p. 3.

> What would be cause for grave concern would be any thought that much of the operation is beyond the ken of the ministry or the Prime Minister; that there are not ministers, elective and responsible members of government, to whom the entire security operation is an open book, who have continuing access to everything that is going on in that area, and who give proper, responsible, political, civilian direction to the operation on a continuing basis.[8]

We would add that not only must responsible Ministers have knowledge of and give direction to security operations, but there must also be means for ensuring that representatives of the opposition parties in Parliament are adequately informed of these activities.

21. Second, the rule of law must be observed in all security operations. Several meanings have been given to this phrase. The meaning which we have in mind is that expressed by the English writer, A.V. Dicey, when he wrote that

> ... here every man, whatever be his rank or condition, is subject to the ordinary law of the realm and amenable to the jurisdiction of the ordinary tribunals... With us every official, from the Prime Minister down to a constable or a collector of taxes, is under the same responsibility for every act done without legal justification as any other citizen.[9]

In our context this means that policemen and members of a security service, as well as the government officials and ministers who authorize their activities, are not above the law. Members of the security organization must not be permitted to break the law in the name of national security. If those responsible for security believe that the law does not give them enough power to protect security effectively, they must try to persuade the law-makers, Parliament and the provincial legislatures, to change the law. They must not take the law into their own hands. This is a requirement of a liberal society. It is, therefore, unacceptable to adopt the view, which we have found expressed within the R.C.M.P., that when the interests of national security are in conflict with the freedom of the individual, the balance to be struck is not for a court of law but for the executive. In very recent years within the R.C.M.P. there has been a view that this conclusion is supported by a 1977 English case, *R.* v. *Secretary of State for the Home Department, ex parte Hosenball:*[10]

> But this is no ordinary case. It is a case in which national security is involved, and our history shows that, when the state itself is endangered, our cherished freedoms may have to take second place.

However, it is misleading to quote this statement out of context. The case concerned an alien whom the Home Secretary ordered to be deported in the interests of national security because he had information that the alien had obtained information for publication harmful to the security of the nation, including information prejudicial to the safety of servants of the Crown. The alien claimed that he was entitled to see the report which was made about him

[8] House of Commons, *Debates*, June 26, 1969, p. 10639.

[9] A.V. Dicey, *Introduction to the Study of the Law of the Constitution*, Tenth edition, London, Macmillan, 1959, p. 193.

[10] [1977] 3 All E.R. 452 at 457.

by a non-statutory advisory Committee which reported to the Home Secretary before the deportation order was made. He contended that natural justice so entitled him. It was in answer to that contention that the above statement was made by Lord Denning, who then continued:

> Even natural justice itself may suffer a set-back... In the first world war, in *R.* v. *Halliday*,[11] Lord Finlay L.C. said: 'The danger of espionage and of damage by secret agents... had to be guarded against.'... But times of peace hold their dangers too. Spies, subverters and saboteurs may be mingling amongst us, putting on a most innocent exterior...
>
> If they are British subjects, we must deal with them here. If they are foreigners, they can be deported. The rules of natural justice have to be modified in regard to foreigners here who prove themselves unwelcome and ought to be deported.

It is thus quite inappropriate to quote what Lord Denning said outside the context of whether the principles of natural justice apply to the exercise of a power to deport, as if it were authority for altering the norms that bind members of the R.C.M.P. when national security is involved.

22. Third, the right of democratic dissent requires that the advocacy of unpopular ideas not be confused with attempts to subvert democracy. A democracy is not liberal unless it permits those of its citizens who seek very basic social, economic or even constitutional change within the democratic system to expound their viewpoint in public and seek adherents to their cause. If citizens who exercise this freedom have their activities noted in secret security dossiers to be used against them by the state, the enjoyment of such freedom is imperilled. The political freedom essential to our democratic system requires that security measures properly distinguish between democratic dissent and true subversion.

23. Those who are responsible for carrying out Canada's security measures must constantly bear in mind that the right to dissent is a constitutional requirement in Canada. This requirement was aptly expressed by Mr. Justice Rand of the Supreme Court of Canada when he stated that under our Constitution

> ... government is by parliamentary institutions, including popular assemblies elected by the people at large in both provinces and the Dominion: government resting ultimately on public opinion reached by discussion and the interplay of ideas.[12]

In a similar vein, Mr. Justice Abbott of the Supreme Court of Canada held that

> The right of free expression of opinion and of criticism, upon matters of public policy and public administration, and the right to discuss and debate such matters, whether they be social, economic or political, are essential to the working of a parliamentary democracy such as ours.[13]

---

[11] [1917] A.C. 260 at 270.

[12] *Saumur* v. *Quebec and Attorney General for Quebec* [1953] 2 S.C.R. 299, at p. 330.

[13] *Switzman* v. *Elbling and Attorney General for Quebec* [1957] S.C.R. 285, at p. 326.

The investigation of security threats by the state must respect this constitutional right to dissent. The exercise of that right must not become an invitation to be spied upon by state security agencies.

24. Canada must have effective security. Security measures have the basic objective of securing our democratic system. The means used to achieve security must meet the requirements of democracy. Effective security within a democratic framework — that is the fundamental precept which has guided our diagnosis of past failures and wrongdoings in Canada's security system, as well as our prescription for reform of the system.

CHAPTER 2

THE ORGANIZATIONAL RESPONSE BY GOVERNMENT

Introduction

1. In the preceding chapter we have set out our understanding of the interests requiring protection by Canada's internal security arrangements. We now describe the institutions through which the Government of Canada has responded to the need for security. We begin with a brief account of the R.C.M.P.'s development as a national police force and then turn to a more detailed account of the historical evolution of the R.C.M.P. Security Service, its current organization and mandate. This is followed by a description of the security and intelligence responsibilities of other branches of the R.C.M.P. and of other departments and agencies of the federal government, and an account of the Cabinet and interdepartmental committee system which co-ordinates and directs the security and intelligence activities of the federal government.

2. This chapter, we must emphasize, is basically descriptive: the analysis and evaluation of events and practices will come later. Here our primary purpose is to provide a factual account of the institutional setting in which the R.C.M.P.'s discharge of its responsibilities for the security of Canada has taken place.

A. THE HISTORICAL CONTEXT AND CURRENT STRUCTURE OF THE ROYAL CANADIAN MOUNTED POLICE

1. The Royal Canadian Mounted Police is a famous and respected national institution. From its beginnings in 1873 and during its earliest days on the western prairies it kept the peace with small numbers of personnel, using careful diplomacy rather than the "triggerhappy" approach with which, rightly or wrongly, law and order are perceived to have been brought to the American frontier. The Force's military structure and practices produced what was seen by the public to be a disciplined corps of dedicated men reputed to be incorruptible and fair. Whether dealing with Indians, settlers, or the highly volatile situation in the Yukon gold rush they had a reputation for administering the law with an even hand and malice to none.

2. The Force was indeed a small organization. Until the end of the First World War, its responsibility was limited to Saskatchewan, Alberta and the Territories: the other provinces were served by provincial police forces. On

February 1, 1920, by Act of Parliament, the Royal North-West Mounted Police absorbed the much smaller Dominion Police, a civilian group that protected federal buildings in Ottawa and hired civilian detectives, and was renamed the Royal Canadian Mounted Police. The Force established small complements in the other provinces although it was far from clear to what extent it would enforce federal laws that by and large had until then been enforced by provincial and municipal authorities. During the period from 1920 to 1950, with the exception of Ontario and Quebec, provinces abandoned their own provincial forces and began the practice, continued today, of contracting with the R.C.M.P. to carry out police duties. After August 15, 1950, when it absorbed the British Columbia Provincial Police, the Force was established as we know it today: an agency of the federal government with a strong presence in the 'contract provinces', the Territories and even in the two provinces, Ontario and Quebec, where it does not have any contractual duties.

3. In all the provinces it is the responsibility of the R.C.M.P. to enforce federal legislation apart from the Criminal Code. In the Territories it also enforces the Criminal Code. The federal government has also assigned the responsibility of protecting the security of Canada to the R.C.M.P. Those two roles have resulted in the R.C.M.P.'s having a significant number of members in each province whose duties are not related to enforcement of the Criminal Code. In addition to those federal policing and security roles, the Force has entered into contracts with provincial and municipal governments to act as the police force for particular regions, enforcing the Criminal Code and provincial and municipal laws. Such contracts exist in all provinces except Ontario and Quebec. In performing their duties under such contracts the R.C.M.P. have a responsibility toward the attorneys general of the various provinces, although the precise nature of that responsibility has not been clearly defined. As of November 1980, total R.C.M.P. strength was made up as follows: 12,864 regular members; 1,527 special constables; 2,089 civilian members; and, 3,757 public servants, making a total of 20,237. Of this total, over 40%, it would appear, are involved in contract policing.

4. In its origin, the Force was military in personnel, structure and orientation. Until after the First World War its members regarded themselves as a military force with the additional powers of peace officers. The Force sent cavalry units to the Boer War, to the western front in 1918 and to Siberia in 1919. While the members were in style a military force, they were intended from the outset to be policemen and (if only because violence by large groups of people seldom erupted in the Canadian west) there were only rare occasions other than for ceremonial purposes when the "horsemen" acted as a military formation. Indeed, after automobiles replaced horses, the cavalry or 'mounted' element became entirely ceremonial.

5. Members acted similarly to members of other police forces in the country, learning the tradecraft and ethics that were developed in London by the professional police force established by Sir Robert Peel in 1829. They learned to interpret the Criminal Code and other federal statutes, and, following the First World War, such increasingly pervasive provincial legislation as the highway traffic acts and statutes first prohibiting and then regulating the sale

and consumption of alcoholic beverages. Until long after the Second World War they were usually the prosecutors in the magistrates' courts in respect of cases investigated by them, for it was not until recent years that in most of the contract provinces the provincial departments of the attorneys general expanded their complement so that lawyers in the departments acted as prosecutors in those courts.

6. In addition to its law enforcement functions the R.C.M.P. accepted the role that other police forces have assumed since Peel's day, which, as stated by the British Royal Commission on the Police, 1962, is as follows:

> ... they have by long tradition a duty to befriend anyone who needs their help, and they may at any time be called upon to cope with minor or major emergencies.[1]

7. In the contract provinces much of the work of the Force in the past has been law enforcement in smaller communities. Large cities in those provinces are policed by municipal forces except in the recently swollen municipalities adjoining the city of Vancouver. They investigated crimes against person and property as well as driving offences and violations of hunting regulations. However, the Force increasingly addressed its attention to the national planning and systematic cooperation with provincial and municipal forces involved in developing programmes to combat the growing international and domestic traffic in narcotics and other drugs, other so-called 'organized crime' including illegal gambling, and 'white-collar crimes' of stock fraud, bankruptcy fraud and even theft of computer-stored information.

8. Moreover, during recent decades, advances in forensic technology, such as new methods of handwriting analysis, serology and ballistics, have demanded increasing investment in personnel and equipment. The need continues for specialized research and development of sophisticated radio communication within the Force and of electronic means of intercepting the communications of suspects.

9. Thus, in addition to 'traditional' police methods, the Force has in recent years been faced with the need to ensure that it has the capacity, in terms of personnel and equipment, to mount investigations employing technology the equal of that employed by police forces in other advanced countries. This need, together with the need to have a security service capable of meeting changing threats, produced an immensely complex problem of evolution for a Force with personnel mostly trained to enforce the law in traditional ways. Many of the problems associated with this evolution are beyond the scope of our terms of reference.

10. Although much of our work has referred to the Security Service, as demanded by paragraph (c) of our mandate, this concentration would be out of focus were we not constantly aware of the historical background and present complexities of the R.C.M.P. as a whole.

---

[1] Cmnd. 1728 at p. 22.

11. Moreover, as we shall point out, some of our observations about the Security Service may well be true of the Force as a whole, and should be taken into account by the Government of Canada and those charged with the future administration of the Force if it is to continue to deserve its reputation as an excellent law enforcement agency.

12. We now wish to summarize the current organizational structure of the Force in order to place in context the more detailed examination of the history and organization of the Security Service which follows in Section B of this chapter.

13. The Commissioner of the R.C.M.P. is appointed by the Governor in Council pursuant to Section 5 of the Royal Canadian Mounted Police Act.[2] That Section provides as follows:

> 5. The Governor in Council may appoint an officer to be known as the Commissioner of the Royal Canadian Mounted Police who, under the direction of the Minister, has the control and management of the Force and all matters connected therewith.

Section 6 of that Act authorizes the Governor in Council to appoint and promote the officers of the Force, the maximum number of such officers to be prescribed by the Treasury Board. By virtue of section 13 of the Act such officers hold office during the pleasure of the Governor in Council. It is the Commissioner's responsibility to appoint all members other than officers (section 7 of the Act), the number again being prescribed by the Treasury Board.

14. Members of the Force are either regular members or 'civilian' members.[3] Civilian members may perform only certain duties.[4] Included in the category of 'regular' members is a group known as 'special constables' who are also limited in the duties which they may perform.[5] In addition to officers and members, the Force has civilian staff "appointed or employed under the Public Service Employment Act" pursuant to section 11 of the Royal Canadian Mounted Police Act. They are employed by the Commissioner.

15. Section 21 of the Royal Canadian Mounted Police Act delegates authority to the Governor in Council and the Commissioner with respect to the organization of the Force. It reads as follows:

> 21. (1) The Governor in Council may make regulations for the organization, training, discipline, efficiency, administration and good government of the Force and generally for carrying the purposes and provisions of this Act into effect.
>
> (2) Subject to this Act and the regulations made under subsection (1), the Commissioner may make rules, to be known as standing orders, for the organization, training, discipline, efficiency, administration and good government of the Force.

---

[2] 1970 R.S.C., ch.R-9.
[3] C.R.C., ch.1391, s.2.
[4] *Ibid.*, s.51(3).
[5] *Ibid.*, s.51(2).

The Governor in Council has prescribed by regulation 3 of the Royal Canadian Mounted Police Regulations[6] that the Force shall be divided into divisions and by regulation 7 that "the organization of the Headquarters of the Force shall be as the Commissioner directs".[7]

16. Those, then, are the legal bases for the structure of the Force from which the following organizational picture emerges.

17. At Headquarters, responsibility below the Commissioner is first divided into four areas, each headed by a Deputy Commissioner or, in the case of the Security Service, the Director General who has Deputy Commissioner status. The four areas are: Administration, Criminal Operations, Canadian Police Services and the Security Service.

18. Both Canadian Police Services and the Security Service are centralized in that all of their operations across the country are controlled directly from Headquarters and the people working in those Services do not report through Divisional Commanding Officers. The rest of the Force's operational components report through the Divisional Commanding Officers, of whom there are 13, each responsible for a geographic division of the Force.

19. Those geographic divisions have essentially the same boundaries as the provinces and the Territories, with the exception of Ontario, which has two such divisions. There are two other divisions not based on geography: the R.C.M.P. Academy 'Depot' Division in Regina, and the Training Division in Ottawa. There are, therefore, 15 divisions in all, and the Commanding Officer of each of them reports directly to the Commissioner. The Deputy Commissioner of Criminal Operations and the Deputy Commissioner of Administration speak on behalf of the Commissioner on specific cases to give direction to the Divisional Commanding Officers (Vol. 6, p. 681).

20. The Commissioner also has seven other components reporting directly to him: the Foreign Services Directorate, the Chief Financial Officer, the Internal Communications Officer, the Public Relations Branch, the Audit Branch, the Planning and Evaluation Branch and his own Executive Officer. An organizational chart of the R.C.M.P. appears in Appendix "U".

21. In the outline of the organization of the Security Service which follows, details of the centralization of the Security Service will be made clear. At this point we simply wish to note that, although an Area Commander of the Security Service, such as, for example, the Saskatchewan Area Commander, reports directly to Security Service Headquarters in Ottawa, he must also keep the Divisional Commanding Officer (in this case "F" Division) informed of any Security Service activities within that Division which might affect the Commanding Officer's ability to carry out his responsibilities.

---

[6] *Ibid.*

[7] *Ibid.*

B. THE R.C.M.P. SECURITY SERVICE: HISTORICAL EVOLUTION AND CURRENT ORGANIZATION

22. The primary function of the R.C.M.P.'s Security Service is to collect, analyze and report intelligence[8] about threats to the security of Canada. A brief account of the historical evolution of the Security Service is instructive: it shows that there has never been a clear and comprehensive public policy on the purpose, methods and structures of security intelligence in Canada. We think that this basic fact may have a good deal to do with the events that have prompted the establishment of our Commission.

The origins of security intelligence

23. Canada's first security intelligence organization was established by Sir John A. Macdonald before Confederation. In 1864 a group of men dressed as Confederate soldiers[9] crossed over the border into Vermont and raided the town of St. Albans. Canadian and British neutrality in the American Civil War was jeopardized. To prevent other such incidents, Macdonald, who was then the Premier and Attorney General West for the United Province of Canada, organized the Western Frontier Constabulary, a small contingent of detectives under the supervision of Gilbert McMicken, a stipendiary magistrate. The main purpose of this force was to collect and report information on "the existence of any plot, conspiracy or organization whereby peace would be endangered, the Queen's Majesty insulted, or her proclamation of neutrality infringed".[10] McMicken's investigators soon had their first threat to contend with: Fenians were drilling and collecting arms in the United States in order to invade the British North American colonies.

24. In 1868, when the Dominion Police Force was established, McMicken became a Dominion Police Commissioner. The primary public role of the Dominion Police was the protection of public buildings in Ottawa, and for this purpose it maintained a small force of about 12 men. However, McMicken continued to supervise a network of undercover agents operating on both sides of the Canada-U.S. border to provide intelligence reports about Fenian activities. When Charles Joseph Coursol, a Montreal Sessions Court Judge, also became a Dominion Police Commissioner, he too supervised a small frontier detective force. As a modern historian testifies, "Macdonald usually knew more about the plans of the Fenians than the Fenians did themselves".[11]

---

[8] The word 'intelligence' in the vocabulary of intelligence agencies refers to information which has been assessed and analyzed for its validity and significance by the intelligence agency. Thus intelligence is distinguished from raw information. We will follow this usage throughout our Report.

[9] The manner of dress is so described in documents in R.C.M.P. files. To the opposite effect Professor Donald Creighton states that the men were Confederate soldiers but were not in uniform: *John A. Macdonald, The Young Politician*, Toronto, Macmillan, 1952, p. 385.

[10] Macdonald Papers, Vol. 234, pp. 100852-4.

[11] Donald Creighton, *John A. Macdonald, The Young Politician*, Toronto, Macmillan, 1952, p. 439.

25. The collection of information and the reporting of intelligence about Fenian threats from 1864 to 1871 was the first security intelligence activity of the Canadian government, but it had many features which were to characterize later activities in this field. For one thing, the methods of investigation were highly secretive. The primary method of collecting information was to infiltrate undercover agents into Fenian organizations. They often spent years within the organization, in some cases working their way into influential positions.

26. Again, the Macdonald papers indicate that the interception of mail and telegrams was another source of information, as was following persons surreptitiously to observe their contacts. The intelligence reports based on information received were sent directly to Ministers, often to the Prime Minister. The Prime Minister, in turn, gave directions to McMicken and Coursol as to the kind of intelligence the government required. Usually the reports were used by the government as a means of assessing the seriousness of the Fenian threat rather than for criminal prosecutions. Intelligence on individual Fenians was used as a basis for screening persons entering Canada or applying for government positions. On occasion reports prompted McMicken to meet with Fenians and their arch opponents, the Orange Lodge, to dissuade them from behaviour which might lead to riotous confrontations.

27. There was no explicit statutory authorization for these secret surveillance activities nor any official statement of government policy with respect to them. Between 1866 and 1873 apparently $133,000 was spent from a Secret Service Fund. These expenditures were not subject to any audit. Allegations of mismanagement of these funds were debated in the House of Commons in 1877 in response to the report of the Select Standing Committee on Public Accounts. That Committee brought forward the first resolution calling for a confidential committee of the House, which would include Opposition members, to review 'Secret Service' matters.[12]

28. One dimension of these early Secret Service activities which was *not* to be an enduring feature of Canada's security intelligence programmes was the collection of information by undercover Canadian agents *outside* Canada. Many of McMicken's undercover agents operated in the United States.

The 1870s to World War I

29. From the early 1870s until the First World War, security intelligence activities at the federal level were much more intermittent. Agents supervised by Commissioners of the Dominion Police continued to play the prime role in collecting information about politically motivated violence in Canada. There were sporadic investigations of Fenian organizations and 'anarchist' episodes (including the dynamiting of the Welland Canal in 1900), but there was no sustained intelligence collection programme. The greatest threat to Canadian security during this period was the North-West Rebellion of 1885. The North-West Mounted Police did not employ undercover agents to collect

[12] *Journals of the House of Commons*, Vol. XI, 1877 Session, Appendix (No. 2). Third Report of the Select Committee on Public Accounts Relating to the Expenditure of Certain Secret Service Funds, p. 10.

security information. Their reports to the government on the insurrection and the need for reinforcements were based on information obtained through their regular police work in the territory.

30. The visit in 1901 of Their Royal Highnesses, the Duke (later King George V) and Duchess of Cornwall, was the first occasion for certain security operations which were to become frequent in the future: V.I.P. protection and countering actions. Percy Sherwood, the Commissioner of the Dominion Police at the time, personally accompanied the royal party on the tour, directed the collection of information by the police about suspected anarchists, and, on one occasion ordered a member of an anarchist group to be detained for the duration of the royal visit.

31. The first time the North-West Mounted Police took on a major responsibility for the collection of security intelligence came in connection with their policing of the Yukon Territory during the gold rush at the turn of the century. Under the direction of Clifford Sifton, Minister of the Interior, and of N.W.M.P. Comptroller Fred White, the N.W.M.P. was asked to investigate rumours of American plots to annex the Yukon territory. Undercover agents, with assistance from the Pinkerton Detective Agency in the United States, conducted surveillance of suspected plotters both in the United States and Canada, and infiltrated American miners' organizations such as the Order of the Midnight Sun. Intelligence reports based on these operations were an important factor in enabling the Canadian government to gauge the seriousness of the threat and take appropriate precautionary measures.

World War I and its aftermath

32. Canada's participation in World War I created the need to investigate and take preventive measures against espionage and sabotage. The manpower resources available to the Government of Canada for this purpose were quite meagre and decentralized. The chief role was played by the small Dominion Police Force which, even after some strengthening during the war, in 1919 reached a total strength of only 140 men. The Dominion Police carried out some investigative work themselves through secret agents, most of whom were hired from American detective agencies, but relied extensively on information collected by police forces across Canada and by officials of the Departments of Customs and Immigration. The situation in British Columbia gives some indication of the decentralized nature of security intelligence activities in Canada during World War I. In that province a former Immigration Agent was appointed a Commissioner of Police for British Columbia under the Dominion Police Act, and was responsible for investigating enemy aliens and suspected pro-German sympathizers. Information collected by his secret agents was reported not only to Dominion Police headquarters in Ottawa but also to the Chief Censor in Ottawa and to British authorities.

33. During the First World War the Royal North-West Mounted Police[13] had the major responsibility for collecting security intelligence in the Prairie

[13] The North-West Mounted Police became the Royal North-West Mounted Police in 1904.

Provinces. Their work in this area stemmed mainly from regulations under the War Measures Act providing for the registration and internment of suspected enemy aliens. Through nearly 200 detachments, they investigated allegations concerning pro-German sympathies and activities of immigrants from Europe. The R.N.W.M.P. did not have a security service division nor had it encouraged the development of plain clothes work for criminal investigations. Consequently, it relied on private detective agencies and secret agents paid with Dominion Police Force funds for undercover counter-espionage investigations. These security agents infiltrated social institutions in immigrant communities, often in response to reports of suspected conspiracies received from citizens. During 1915 alone, the Mounted Police and their agents made 2,309 individual investigations resulting in the internment of 396 persons. After Saskatchewan and Alberta took over responsibility for provincial policing in 1917, the R.N.W.M.P. closed most of its detachments in these provinces and concentrated on preventing German agents from crossing the border into Canada.

34. Throughout the war, Commissioner Perry directed Canadian security investigations in the United States from R.N.W.M.P. Headquarters in Regina. The American authorities were not always notified. At this time there appeared to be no jurisdictional limits for 'friendly foreign agencies'. Just as Canada conducted security operations in the United States, the British ran agents in Canada without informing the Canadian government. At times this led to embarrassment. In 1917, for instance, the British Navy intercepted the Bolshevik leader Leon Trotsky off the coast of Nova Scotia on his way home to Russia after the abdication of the Czar, and, without consulting Ottawa, had him interned in that province. The Canadian authorities were unhappy about the Admiralty's action, and were relieved when Trotsky was allowed to continue his journey some three weeks later.[14]

35. In the period of social dislocation, economic instability, and political upheaval which followed World War I, federal security intelligence agencies focussed on what was perceived to be a new threat to Canada's internal security: radical labour agitation — especially in Western Canada. At this time security intelligence work at the federal level was far from unified. By the fall of 1918 the federal government was receiving reports from four security agencies. Security intelligence was collected in Saskatchewan and Alberta by the Mounted Police, whose Commissioner reported to the President of the Privy Council, and in the other provinces by the Dominion Police, whose Commissioners were responsible to the Minister of Justice. In addition, the Chief Censor's Office and a Directorate of Public Safety, established in the Justice Department, supplied the government with assessments of the internal security threat. The Cabinet feared that the post-war labour agitation was nurtured by revolutionary international forces and directed the security agencies to investigate these international connections. Both the Dominion Police and the R.N.W.M.P. carried out extensive undercover investigations into the labour movement. Although intelligence reports from R.N.W.M.P. Headquarters do not appear to have corroborated the politicians' fears of internationally

[14] William Rodney, "Broken Journey: Trotsky's Canada", 1917. *Queen's Quarterly*, Winter, 1967.

inspired revolutionary plots, Ministers continued to assess the situation differently, partly on the basis of assessments of the internal security threat received from British sources.[15] In his memoirs Sir Robert Borden described the Winnipeg General Strike of 1919 as "a definite attempt to overthrow the existing organization of the government and to supercede it by crude, fantastic methods founded upon the absurd conceptions of what has been accomplished in Russia".[16]

The development of security intelligence as an R.C.M.P. responsibility: 1920-46

36. The Dominion Police Force was absorbed into the Mounted Police under legislation which came into effect on February 1, 1920. The Royal Canadian Mounted Police was now a national police force with federal law enforcement responsibilities. One of the principal purposes of this change was to unify and strengthen the federal security intelligence capability.

37. Although the R.C.M.P. was now the sole federal agency responsible for the collection of security intelligence there were neither statutory nor ministerial guidelines for carrying out this intelligence role. In the parliamentary debate on the R.C.M.P. Act no mention was made of the Force's security intelligence role. In the decades between the wars, government direction was provided informally through frequent meetings between the Minister of Justice (who was responsible for the R.C.M.P.) and the Commissioner of the R.C.M.P., and through the response of Ministers to weekly and monthly intelligence reports from the R.C.M.P. Until 1933 a senior civilian employee of the Force, who was often referred to as Director of Intelligence, was chiefly responsible for liaison with government departments on security intelligence matters.

38. From 1920 until the establishment of the R.C.M.P.'s Special Branch in 1946, security service activities were the responsibility of the Criminal Investigation Branch (C.I.B.) of the R.C.M.P. Until the mid-1930s there was little to differentiate security investigations from other investigative work of the C.I.B. At Headquarters, the Director of Criminal Intelligence was responsible for security and intelligence investigations. In the field, C.I.B. detectives investigated alleged subversives as well as criminal cases. A secret agent who had penetrated a subversive group reported to C.I.B. detectives, or, if the agent was a member of the Force, to the Director of Criminal Intelligence at Headquarters. In 1936 a distinct 'Intelligence Section' in the C.I.B. was established at Headquarters.

39. On the eve of World War II, although some specialization of security intelligence activities had begun to develop both at Headquarters and in the field, the number of R.C.M.P. members involved in these activities was extremely small. The Headquarters group involved in security intelligence

---

[15] S.W. Horrall, "The Royal North-West Mounted Police and Labour Unrest in Western Canada, 1919", *Canadian Historical Review*, Vol. 61, LXI, No. 2, June 1980.

[16] *Robert Laird Borden: His Memoirs*, Toronto, Macmillan of Canada, 1938, Vol. II, p. 972.

work consisted of only six persons, some of whom were part-time. The senior intelligence officer, Inspector C.E. Rivett-Carnac, for example, was also the editor of the *R.C.M.P. Quarterly*.

40. World War II significantly increased the security intelligence responsibilities of the R.C.M.P. and led to a rapid expansion of the Intelligence Section. At its peak in 1943 the strength of the Intelligence Section at Headquarters had grown to three officers and 95 others. Similarly the field Divisional Headquarters developed units specializing in security work, especially the analysis of information obtained from internees. The largest of these units were in Toronto (20), Montreal (19) and Vancouver (9). By the end of the war the scale of specialized security intelligence work within the R.C.M.P. had contracted considerably.

41. In the years between the wars R.C.M.P. security intelligence activities were almost entirely centred on counter-subversion. The main targets were Communist groups and Communist-led labour organizations. Successive governments wished to be kept informed about the possibility of revolutionary plans and international sources of support of such organizations. To obtain this information the R.C.M.P. frequently had its own members infiltrate the organizations. In a number of cases, these R.C.M.P. members remained undercover for years as active members of Communist organizations. However, section 98 of the Criminal Code, which was enacted in response to fear engendered by the 1919 Winnipeg General Strike, made membership in such organizations a criminal offence.

42. In the 1930s, as a result of co-operation between the federal and Ontario governments, the Ontario government decided to prosecute six leading members of the Communist Party for offences under section 98. An R.C.M.P. undercover agent gave evidence at the trial and in so doing disclosed the nature and extent of R.C.M.P. penetration of the Communist movement in Canada. The six leaders were found guilty of offences relating to their membership in the Party but were acquitted of the more serious charge of acting in a seditious manner to overthrow the state. The trial stimulated opposition to section 98 of the Criminal Code, and, following a change of government in 1935, section 98 was repealed. Following these events, some curtailment of undercover activity occurred.

43. One consequence of this focus on Communist political groups and labour organizations was that the R.C.M.P.'s involvement in security intelligence activities became a subject of political controversy, and frequent criticisms were voiced in the House of Commons about suspected R.C.M.P. surveillance of left-wing political activity. No official explanation of these activities was provided by Ministers; indeed, it was not until 1934 that a Minister of Justice reluctantly acknowledged in Parliament that there was a 'secret service' within the R.C.M.P.

44. The rise to power of Hitler and Mussolini was followed by the formation of Fascist and Nazi political organizations in Canada. In the latter part of the 1930s, these organizations became a major target of R.C.M.P. surveillance. Information obtained about membership in such organizations was of great

importance in identifying suspected saboteurs immediately after war was declared in September 1939. Besides using informants and undercover agents, the R.C.M.P. intelligence section used 'wire supervision' (the interception of telephone calls) for the first time in the late 1930s as a means of gathering information about suspected subversive organizations. There was no statute making such a technique a crime at that time.

45. When the R.C.M.P. became responsible for the collection of security intelligence in 1920, it adopted the policy of restricting the covert operations of R.C.M.P. intelligence personnel to Canada's territorial limits. There is no evidence that this policy was the result of a conscious decision by the Canadian government. Nonetheless, it reversed the practice which Canada had followed in the past, and it is now government policy. It meant, in effect, that Canada, unlike her major allies, did not develop a capacity for using secret means to collect in foreign countries information pertinent to Canada's security or national interests. It also meant that the only way of obtaining foreign information relevant to Canada's internal security and not available through open sources was from 'friendly' foreign agencies. Consequently, during the inter-war years the R.C.M.P. took steps to develop a liaison relationship with British and American intelligence agencies. As World War II approached, arrangements for sharing intelligence with the F.B.I. and the British secret agencies were strengthened.

46. During World War II the national security functions of the R.C.M.P. were considerably expanded. As in the 1914-1918 war, the largest intelligence function was in relation to the registration and internment of enemy aliens. The Commissioner of the R.C.M.P. was appointed Registrar General of Enemy Aliens and 16,000 Germans were registered by March 1940. When Italy entered the war in June 1940, R.C.M.P. files permitted the rapid identification, arrest and detention of Italian immigrants suspected to be dangerous to the security of Canada. Fear of undercover enemy agents led to continual reports by suspicious citizens, and each case was investigated by a member of the Intelligence Section. By March 1941, all Canadian residents of Japanese citizenship who had not become Canadian citizens by 1922 were registered. R.C.M.P. intelligence reports indicated that only a small number of these persons were security threats. However, after the outbreak of war with Japan, in response to strongly expressed public apprehension, the government, using powers available to it under the War Measures Act, relocated all Japanese Canadians from the West Coast to inland areas and detained them there, and confiscated their property.

47. Another security intelligence function assigned to the R.C.M.P. during the war was to advise about industrial and military sites within Canada which might be vulnerable to sabotage. A special subsection of the Intelligence Section was established for this purpose.

48. The R.C.M.P.'s counter-espionage activities during the war were not extensive, perhaps because the large internment programme may have deprived enemy agents of Canadian contacts. In the early years of the war, before the Soviet Union became an ally, the prime target of counter-subversion activities

was suspected Communist attempts to disrupt the war effort. Surveillance was also maintained on the anti-conscriptionist movement in Quebec and on the Jehovah's Witnesses. The latter group, like the Communists, had been declared an illegal organization under the Defence of Canada Regulations.

The expansion of security intelligence activities after World War II

49. In 1945 the revelations of the Soviet cypher clerk, Igor Gouzenko, created a turning point in the development of Canada's security intelligence activities. Gouzenko revealed that the Soviet Union had organized an extensive espionage network in Canada. This network operated largely through the 'recruitment' of civil servants and scientists into Communist front groups and Communist Party cells. Members of the network, through their positions in government departments and research agencies, had obtained and passed over to their Soviet 'handlers' information of vital importance to the defence of Canada and her allies. These disclosures alerted the Canadian government, as well as the British and American governments, to the urgent need to strengthen their defences against Soviet espionage and clandestine Communist involvement in political life.

50. In 1946, in direct response to the Gouzenko spy revelations, the Canadian government introduced a programme of security screening in the federal Public Service to ensure as far as possible that persons with access to secret information were trustworthy. Such a screening programme was one of the main recommendations of the Royal Commission on Espionage which had investigated the Gouzenko disclosures. The Commissioners were Mr. Justice Robert Taschereau and Mr. Justice R.L. Kellock of the Supreme Court of Canada. Under the screening programme the R.C.M.P. was designated as the agency responsible for investigating the personal lives and political associations of persons requiring security screening. Government departments would decide whether to grant or deny clearance largely on the basis of R.C.M.P. reports.

51. The security screening work of the R.C.M.P. has been authorized by a series of Cabinet Directives. These Directives have established criteria for identifying the kinds of political activity which, in the government's view, represent threats to the security of Canada. Originally these criteria specified membership in or association with Communist or Fascist organizations as the basis for denying a security clearance. But over the years these criteria have been widened to embrace more generic categories of political activity. Cabinet Directive 35, which since 1963 has governed the security screening of government employees, sets out the criteria of 'disloyalty' and 'features of character' which it is considered might severely affect a person's 'reliability'. Greed, debt, illicit sexual behaviour, drunkenness, drug addiction and mental imbalance are listed as examples of 'unreliability'. In 1972 the Security Advisory Committee authorized the R.C.M.P. to include in its security screening reports information on a candidate's "separatist sympathies, associations and activities". This formalized an R.C.M.P. practice which had arisen out of an arrangement made between the R.C.M.P. and the Privy Council Office seven years earlier.

52. In Part V and Part VII of this Report we will examine in detail the policy issues associated with these criteria. Here we wish to note the impact these

criteria have had on the surveillance and investigative work of the security side of the R.C.M.P. The Security Service systematically collects and stores information on individuals and groups who fall within these criteria. This provides the basic data for 'subversive indices' checked by the security screening branch for every person who is screened. Beginning in 1946, the systematic collection of information about Canadians who fall within the security screening criteria has been a major function of the security intelligence division of the R.C.M.P. Yet, until 1975, the Cabinet Directive on security screening for the federal Public Service was the only written instruction from the Cabinet concerning the kinds of security intelligence to be collected by the R.C.M.P.

53. Three other security screening programmes came to rely heavily on the R.C.M.P. for security intelligence. These were for citizenship, certificates of identity (i.e. travel documents for non-citizens) and immigration. Of these three, the immigration screening programme had the greatest impact on the R.C.M.P. The Immigration Act of 1952 established "prohibited classes" of persons who were to be refused admission to Canada on security grounds. Some modifications in these criteria were made when the new Immigration Act[17] was passed in 1976. Section 19(1) of the new Act set the criteria for excluding persons from entry to Canada on security grounds. The R.C.M.P. established a visa control section to assess the extent to which each of the thousands of post-war refugees wishing to emigrate to Canada might fall within the prohibited categories of the Immigration Act. The establishment of this section led for the first time to the posting abroad of R.C.M.P. members to serve as visa control officers.

54. Another government security programme in the post-war years, which added to the security intelligence mandate of the R.C.M.P., was aimed at preparing lists of persons to be interned in the event of an emergency. This programme was originally based on the Defence of Canada regulations passed pursuant to the War Measures Act during World War II. These regulations were revised in 1959-61 and replaced by the draft Internal Security Regulations. The draft regulations are designed to be used if a proclamation is issued invoking the War Measures Act. They provide that the Minister of Justice may order an individual or group of individuals to be interned and the Governor in Council may declare a group to be an illegal organization. The R.C.M.P.'s role in the preparation for internment has been to provide information on individuals and groups to an Advisory Committee on Internment which was appointed by the Department of Justice. The Committee, on the basis of established criteria, decided which names to put on the internment list. In the atmosphere of the Cold War, the focus was on the Communist Party and Communist front organizations. This programme was given a high priority by the R.C.M.P. until the mid-1960s.

55. The increased security intelligence functions assigned to the R.C.M.P. after World War II led to a more specialized organizational structure within the R.C.M.P. In 1946, the Intelligence Section, which at Headquarters had been part of the Criminal Intelligence Branch, was organized into a Special

[17] Immigration Act, 1976, S.C. 1976-77, Vol. 1, ch.52.

Branch. Four years later the Officer in Charge of the Special Branch, Superintendent McClellan, began to report directly to the Commissioner of the R.C.M.P. rather than to the Director of the Criminal Investigation Branch. In 1956, the Special Branch was elevated to the Directorate level and became known as the Directorate of Security and Intelligence or "I" Directorate. Assistant Commissioner Harvison (who, like Superintendent McClellan, would later become a Commissioner of the R.C.M.P.) was the first officer in charge of this Directorate. This structure remained intact until 1970. In that year, the new head of "I" Directorate, John Starnes, was appointed Director General, with a rank equivalent to that of Deputy Commissioner, and the name of "I" Directorate was changed to the Security Service, underlining the difference between security intelligence work and regular police work.

56. The number of persons involved in the R.C.M.P.'s security intelligence work increased rapidly in the years following World War II. From the small group at Headquarters, which constituted the Intelligence Section at the end of World War II, Special Branch had grown considerably by 1951. By 1960, "I" Directorate's membership had tripled and had doubled again by the time Mr. Starnes took over as Director General a decade later. In a little over 20 years, the R.C.M.P.'s manpower specializing in security intelligence activities had increased more than fifty-fold.

57. Not all of those in the R.C.M.P.'s Special Branch and its successors, "I" Directorate and the Security Service, have been regular members of the R.C.M.P. Since 1951 there have been four different categories of personnel which reflect the make-up of the Force as a whole:

— Regular Members of the R.C.M.P.

— Special Constables of the R.C.M.P.

— Public Servants

— Civilian Members of the R.C.M.P.

The largest component of the Security Service is made up of regular members of the R.C.M.P. who have joined the Force as young men (there have been only two women), have gone through the basic training at Regina, and at different points in their career have moved over from regular police work to the part of the Force which does security intelligence work. Since 1951 regular members of the R.C.M.P. have constituted at least 44 per cent of the personnel on the security side. Special constables have been recruited into the Security Service to perform specialized investigative work and are not on the career path of a regular R.C.M.P. member. The public servants carry out support staff functions such as clerical and stenographic work and are drawn from the staffing pool of the Public Service.

58. The fourth category of security intelligence personnel — the civilian member — is of particular importance for it is the effective melding of this component into the security intelligence team that has created a severe organizational challenge. The R.C.M.P. began to recruit civilian members into the Special Branch as Reader Analysts in the early 1950s. Their primary role was to analyze information from the field and to write intelligence reports for

Ministers and government departments. The intellectual and literary skills of these civilian members could be of crucial importance for the quality of intelligence reports, but as outsiders their career prospects in security intelligence work were dim. This was soon identified as a serious organizational problem. In 1957, Deputy Commissioner Brunet, writing to the Commissioner about general conditions in "I" Directorate, made this comment:

> The situation as regards Reviewer Analysts is a problem and a source of worry at times. As you know, they are all civilians and, there not being much future for them, with a few exceptions we have not been able to keep these people very long and they are hard to replace. We never know which one may go next.

Later on in this Report we shall analyze this problem in detail and consider the various attempts to deal with it. But in this historical overview we wish only to note that this major problem in the organization of Canada's security intelligence capability, a problem which still exists today, first surfaced nearly 25 years ago.

59. While the security screening programmes provided the basis for routine security intelligence collection and reporting by the R.C.M.P., there was also a steady expansion after World War II and until the early 1970s, of R.C.M.P. investigative and preventive activities with respect to both foreign intelligence agencies in Canada and various forms of domestic 'subversion'. There was no explicit administrative or statutory authorization for this expansion. We have previously noted that the original R.C.M.P. Act of 1920 made no explicit reference to the security intelligence responsibilities of the Force and nothing has been added to the R.C.M.P. Act since then. The only specific reference to security intelligence activities is to be found in section 24 of the R.C.M.P. Regulations,[18] which lists the following amongst the duties of the Force:

> (e) to maintain and operate such security and intelligence services as may be required by the Minister.

Subsequent parts of this Report will describe a number of the operations carried out in recent years by the Security Service and will analyze the legal and policy issues arising from them. The following is simply an outline of the main features of security operations as they developed since World War II.

60. Following the Gouzenko revelations, the R.C.M.P.'s counter-intelligence operations (efforts to detect and prevent activities of foreign intelligence agents in Canada) increased in scale and sophistication. By the end of World War II all of the major powers and a number of lesser countries had developed very substantial secret services to gather intelligence and promote their national interests in foreign countries. The relaxation of international tensions in the détente period did not lead to an abatement in the 'secret war'. Although Canada did not develop an espionage capacity of its own, there was no indication that Canada was regarded as 'off limits' by the foreign intelligence agencies of other countries. A major security intelligence role of the R.C.M.P. has been the responsibility for keeping track of these foreign intelligence activities in Canada and of taking certain preventive actions against them.

[18] C.R.C., ch.1391.

61. The vocabulary of counter-intelligence distinguishes 'legal' from 'illegal' operations. There is no consistency within the intelligence community as to precise definition of what is a 'legal' agent and what is an 'illegal' agent. One distinguishing factor is that the 'legal' agent is one who operates under diplomatic cover out of his mission, while an 'illegal' is an agent who operates independently under deep cover, often with false identity documents, and sometimes communicates directly with the intelligence headquarters of the country which he serves. R.C.M.P. counter-intelligence investigations have been concerned with detecting the activities of both kinds of agents. This has involved the surveillance of diplomats suspected of carrying out secret intelligence functions in Canada as well as the investigation of persons suspected of being long-term, deep cover foreign agents.

62. Foreign intelligence agents, whether 'legal' or 'illegal', are usually highly trained in evading detection. The 'tradecraft' of espionage which developed during World War II was continually refined in the post-war years, thereby creating pressure on counter-intelligence agencies to keep pace. The counter-intelligence branch of the R.C.M.P. made considerable efforts to increase its technical competence in detecting and countering foreign intelligence agencies. Among other things, this led to an increased use of technical means of intercepting oral and written communications, technical visual surveillance and the use of mobile physical surveillance teams. Efforts to detect 'illegals' also led to the use of confidential personal information to check individual identities. In Part III of this Report we shall be reporting on the legal implications of these techniques; in Part V we shall put forward our recommendations on the laws, policies and procedures which should govern the use of these techniques.

63. Counter-intelligence operations have been concerned not only with collecting information about foreign intelligence activities but also with preventing such activities. In a number of cases, R.C.M.P. investigations led to prosecutions of individuals for espionage offences under the Official Secrets Act or decisions of the Government of Canada to declare foreign diplomats *personae non gratae* and expel them from Canada. Since World War II there have been 20 cases involving persons charged with espionage offences under the Official Secrets Act (see paragraphs 9 to 19 of our First Report for a discussion of these cases) and 42 diplomats have been declared *personae non gratae*. But considerably more frequent are less formal preventive actions such as warning Canadians who are in danger of being compromised or recruited by foreign intelligence agents. The rarest but most valued preventive activity is the 'turning' of a member of a foreign intelligence agency into a 'double agent' of the counter-intelligence agency. Like counter-intelligence agencies in all countries, the R.C.M.P. counter-intelligence service has expended much energy on preventing the development of double agents in its own ranks and developing double agents within 'hostile' intelligence agencies.

64. In the immediate post-war years, the Soviet Union's intelligence activities in Canada were the major 'target' of the R.C.M.P.'s counter-intelligence work. More recently, while the Soviet Union has remained a target, considerable investigative resources have also been directed towards the agents of a number

of other countries as well as a number of organizations and certain countries associated with international terrorism.

65. 'Foreign intelligence' activity investigated by the R.C.M.P. has often had little to do with espionage as that term is normally understood. Much of it has taken the form of what in the jargon of counter-intelligence is known as "active measures of foreign intervention". Such measures include, for example, efforts to induce members of an immigrant community in Canada to support the government of their native land and efforts to induce a Member of Parliament or a senior official of the Canadian government to support the interests of a foreign government in Canadian policy-making. Foreign intelligence programmes of this kind in Canada are apt to embrace activities which are well within the ambit of acceptable diplomatic activity or lobbying as well as activities which involve stealth and blackmail and clearly go beyond conduct compatible with the values of Canadian society and its system of government. In Part V of this Report we shall discuss the principles which should apply to counter-intelligence investigations against active measures of foreign interference. In this brief historical survey we wish only to report that in the last two decades active measures of foreign interference have been of increasing concern to the security intelligence arm of the R.C.M.P. and that no clear policies or procedures have been developed by the government for identifying which kinds of foreign intelligence activities are legitimate targets of investigation and which are not.

66. The surveillance and investigation of domestic subversion by the R.C.M.P. also increased greatly in the post-war years. Earlier, in the years between the two World Wars these counter-subversion investigations focussed on Communist organizations and suspected Communist front organizations. The Gouzenko spy trials and the political atmosphere of the Cold War encouraged concentration in these areas. However, in the 1960s, R.C.M.P. counter-subversion activity began to extend far beyond Communist groups.

67. One of the major new concerns was terrorism. In one sense terrorism was not new — in the 19th century and early 20th century, Canada had contended with groups such as the Fenians and "anarchists" who used violence for purposes of political propaganda or to force concessions from government. What was new in the 1960s was the scale, the intensity and the publicity associated with terrorism. The terrorist groups which have emerged in the last two decades have had much more money and much more help from foreign governments than was ever the case in the past. They have also taken advantage of the freedom of movement and relative permissiveness of liberal democracies such as Canada. In particular they have relied on the mass media to derive the maximum political impact from an act of violence. As one historian of terrorism has put it, they have learned

> that the terrorist act by itself is next to nothing, whereas publicity is all.[19]

68. A major responsibility of the R.C.M.P.'s "I" Directorate and its successor, the Security Service, in the 1960s and 1970s has been the investigation of

---

[19] Walter Laqueur, *Terrorism*, London, Weidenfeld and Nicholson, 1977, p. 223.

domestic terrorist organizations, especially those like the Front de Libération du Québec (F.L.Q.) in Quebec. The 1970 October Crisis increased the priority given to the need for good intelligence about terrorist threats in Quebec. Prime Minister Trudeau subsequently told the House of Commons that after

> . . . the events of October 1970, when there had been terrorism, murder and kidnapping, we directed the R.C.M.P. — and I believe this was the will of the House — to pay a little more attention to internal subversion caused by ideological sources in Canada and not only concentrate on externally sponsored types of subversion.
>
> It then became obvious that one of the groups they were going to look at was one composed of those who were trying to break this country, separate it, and who had been using force in order to do it. There was a great deal of indignation on the part of members opposite, and indeed many people across the country, because at the time of the October, 1970, events the police had to throw a very wide net indeed and arrest many people who were apparently guilty of nothing because the police were misinformed. They did not have inside information on the terrorists, those who had kidnapped Mr. Cross and Mr. Laporte. So obviously we told them — we did not have to tell them because they would have done it by themselves — to concentrate a little more on this threat. So I suppose that as a result of that they began infiltrating the F.L.Q. and they began trying to get more information on those who would destroy the country by force, whether they be in Quebec or in other parts of the country.[20]

A number of the events examined and reported upon by our Commission are related to the efforts of the R.C.M.P. Security Service to obtain intelligence about terrorist organizations in Quebec.

69. Intelligence concerning the activities of foreign terrorists also became a major priority of the Security Service in the 1970s. The tragic terrorist assault on the Munich Olympics in 1972 and the awarding of the 1976 Olympics to Montreal highlighted the importance to Canada's security of prompt and accurate intelligence about foreign terrorist organizations. Largely through the Security Service, Canada has been both a consumer and a producer of international intelligence about terrorism. Canada's obligation to contribute to the international pool of intelligence about terrorist groups was strengthened in 1974 when Canada signed the United Nations' Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents.[21]

70. The terrorist component of R.C.M.P. counter-subversion investigations has been the least controversial element in the expansion of counter-subversion activities. Much more contentious has been the investigation of 'radical' or 'extremist' groups, many of which do not participate in political violence. Student radicalism of the mid- and late-1960s and the so-called 'New Left' became areas of concern to the R.C.M.P., as did native and black 'extremism'. Exponents of Quebec independence using democratic means to promote their

---

[20] House of Commons, *Debates*, November 2, 1977, p. 564.

[21] Resolution adopted by the General Assembly A/RES/3166 (XXVIII), February 5, 1974.

political objectives, a number of trade unions, and Canadian supporters of the anti-Viet Nam war movement, among others, became targets of security intelligence surveillance by the R.C.M.P.

71. In Part V of this Report we shall analyze in some detail past policies with respect to the targetting of domestic subversion and advance our own recommendations as to how domestic subversion should be defined as a legitimate area of surveillance. Here we wish only to record the general growth of domestic subversion investigation by the R.C.M.P. in the 1960s and '70s and the fact that at that time there was no clear basis in law or government policy for determining the proper scope of counter-subversion investigation by the R.C.M.P. Aside from the criteria of 'disloyalty' set out in the Cabinet Directive governing security clearance, there were no government guidelines as to where legitimate dissent ended and subversion began.

72. Outside the terrorist field, counter-subversion investigation resulted in few criminal prosecutions. Some of the information collected was used as a basis for advising police forces of the participation of members of 'subversive' organizations in political demonstrations and picketing. Intelligence about 'subversive' organizations was also used to advise those responsible for protecting vital points and V.I.P.s, and for providing security for major international events in Canada such as the Habitat Conference and the Olympic and Commonwealth Games. Information was also passed on to federal government departments for a variety of purposes. Often information about members of 'subversive' organizations was reported as provided for under the legislation and directives governing security screening programmes. On other occasions reports were designed to advise departments as to the presence or absence of 'subversives' in activities of concern to the departments. One example of such a report was an R.C.M.P. brief on the "Extra Parliamentary Opposition" which was sent to the Solicitor General on May 12, 1971, the policy implications of which we shall examine in subsequent chapters.

73. As with counter-intelligence activities, the R.C.M.P.'s counter-subversion operations were not confined to collecting and reporting information. A wide range of 'countering' measures were employed to disrupt or break up groups considered to be subversive. We have inquired into the nature of these measures and have heard a great deal of evidence about their use especially in the 1970s. In Part III we shall report on those countering techniques which were not authorized or provided for by law and in Part V we shall analyze the full range of countering techniques and present our recommendations with regard to their use.

74. Throughout the period of expanded counter-subversion activity, the Security Service relied mainly upon the collection of information from covert rather than overt sources. The primary information on which its intelligence reports have typically been built has been garnered from investigations using clandestine investigative techniques. Many of these techniques were originally developed for counter-intelligence work against secret foreign agents. In the 1960s and 1970s they were increasingly used against Canadian citizens and organizations suspected of subversive activities. Our Report will indicate later the

extent to which electronic surveillance, mail opening, searches without warrant and the use of confidential personal information have been used in the counter-subversion and in the counter-intelligence spheres. 'Human sources' tended to be used to a greater extent in counter-subversion activities than in counter-intelligence operations. Paid informants and undercover members of the Security Service have been frequently used as a means of obtaining information about the membership, plans and activities of domestic political groups suspected of being involved in subversive activities.

75. While in the years between the end of World War II and the appointment of the Royal Commission on Security in 1966 the security intelligence activities of the R.C.M.P. were increasing rapidly, both in volume and in the use of intrusive investigative techniques, there was relatively little change in governmental arrangements for directing or reviewing this activity. Parliament still played no active role in either approving or reviewing security intelligence activities. On the executive side, the Prime Minister continued to have the ultimate responsibility for matters relating to national security, and the Minister of Justice continued to be the Minister responsible for the R.C.M.P., but there were no established procedures whereby either was kept informed on a regular or systematic basis of the scope of R.C.M.P. security intelligence activities or the methods employed in these investigations.

76. In the early 1960s, as security issues became increasingly controversial, it was the Prime Minister who most often took the chief responsibility for responding to Opposition questions in the House of Commons and stating government policy. On October 25, 1963, Prime Minister Lester B. Pearson, responding to public concerns about security investigations, announced in the House of Commons changes in security clearance procedures. These procedural changes were designed to provide some safeguards to government employees by requiring that doubt about their security status be disclosed to them and that a panel of senior officials review cases in which departments were proposing to deny a security clearance. Later, in November 1963, in response to concerns voiced by the Canadian Association of University Teachers, Prime Minister Pearson issued the following policy statement with respect to R.C.M.P. surveillance of university campuses:

> There is at present no general R.C.M.P. surveillance of university campuses. The R.C.M.P. does, in the discharge of its security responsibilities, go to the universities as required for information on people seeking employment in the public service or where there are definite indications that individuals may be involved in espionage or subversive activities.[22]

It is worth noting that this was the only occasion during this period when the government publicly disclosed policy in relation to the R.C.M.P.'s gathering of security intelligence.

---

[22] "R.C.M.P. Activities on University Campuses", *C.A.U.T. Bulletin*, Vol. 13, No. 2, October 1964.

The Royal Commission on Security and its implementation

77. On March 7, 1966, Prime Minister Pearson announced the establishment of the Royal Commission on Security, popularly referred to as the Mackenzie Commission after its Chairman, Mr. Maxwell Mackenzie. Mr. Yves Pratte and the Honourable M.J. Coldwell were Mr. Mackenzie's fellow Commissioners. Although the decision to establish the Commission had been triggered by public controversy surrounding the case of Mr. George Victor Spencer, a postal employee dismissed for security reasons, the Commission's terms of reference went far beyond this case and directed it "... to make a full and confidential inquiry into and report upon the operations of Canadian security methods and procedures".

78. Mr. Pearson linked the Commission's mandate to the establishment of the Department of the Solicitor General. Under the Government Organization Act, 1966, the Solicitor General of Canada took over the duties and functions previously exercised by the Minister of Justice with respect to penitentiaries, parole and the R.C.M.P. The Prime Minister emphasized the importance of the security work amongst the responsibilities of the newly created Department. He told the House of Commons that "... a high priority function of the new Department will be to examine in detail the problems of espionage and subversive activities, and to determine how best to deal with them". It was, he said, "in order to assist the Solicitor General in his particular and new responsibility..." that the government had decided to establish the Commission.[23]

79. The Royal Commission on Security submitted its Report to the government in October 1968, and the government published an abridged version in June 1969. We have had the opportunity of comparing the abridged and unabridged versions and would note that very little was deleted from the published Report. Most of the Commission's recommendations dealt with ways and means of improving government security procedures in such matters as security screening, departmental security and industrial security. We shall be referring to many of these recommendations in Part VII of this Report.

80. The Royal Commission also recommended three important structural changes in Canada's security system. First, it called for the establishment of a Security Secretariat in the Privy Council Office to formulate and supervise the implementation of security policy and procedures. Second, and most importantly for the R.C.M.P. Security Service, it recommended the establishment of a civilian agency outside the R.C.M.P. "... to perform the functions of a Security Service in Canada".[24] And third, the Commission called for the establishment of a Security Review Board to hear appeals in security screening cases affecting the Public Service, immigration and citizenship. The Board would also receive periodic reports from the Head of the Security Service and "have authority to draw to the direct attention of the Prime Minister any matters it considers appropriate."[25]

---

[23] House of Commons, *Debates*, March 7, 1966, pp. 2296-97.

[24] *Report of the Royal Commission on Security*, paragraph 297.

[25] *Ibid.*, paragraph 66.

81. The Commission did not contemplate any significant change in the new Security Service's mandate from that of the R.C.M.P. Security Service. Its primary role would continue to be the collection, evaluation, and reporting of information or intelligence "concerning espionage and subversion".[26] The Royal Commission also recommended that future legislation should provide for the interception of telephone conversations, electronic surveillance and the examination of mail for security purposes.[27]

82. The government did not accept the Royal Commission's recommendation to establish a civilian Security Service separate from the R.C.M.P. Instead, it opted for something of a compromise. In tabling the Commission's report in the House of Commons in June 1969, Prime Minister Trudeau announced that the Security Service would remain under the Commissioner of the R.C.M.P. but it would become "increasingly separate in structure and civilian in nature". Under new and more flexible policies relating to recruiting, training and career planning, it would be possible, according to the Prime Minister, for

> . . . an increasing number of university graduates from all parts of Canada to join the [Security Service] in a civilian capacity and to aspire to positions at the top of that organization.[28]

In Part VI of this Report, we provide a detailed account of the extent to which Prime Minister Trudeau's policy was implemented. Here we will record only the highlights.

83. So far as 'civilianization' is concerned, the most dramatic development was the appointment of persons who were not R.C.M.P. members as Directors General of the Security Service: first, Mr. John Starnes from the Department of External Affairs who served from January 1, 1970 to April 30, 1973, and then Lieutenant-General Michael Dare from the Department of National Defence, who has served from May 1, 1973 until the present. But aside from these appointments there was little progress towards the Prime Minister's objective. Between 1969 and 1979 the civilian member component increased from 9.9 to 17.2 per cent of the Security Service's strength, but nearly all of the increase has been at the lower ranks or in the service and administrative branches. By the end of the decade not a single civilian was in an officer-equivalent position in an operational or planning branch. However, programmes to assist R.C.M.P. members in returning to university have substantially raised the formal education levels of Security Service members since 1969.

84. As for autonomy, there was little change until 1976 when the Security Service was given "National Division" status within the R.C.M.P. This meant that more administrative responsibilities were delegated to the Director General of the Security Service and, operationally, Security Service field units would report to Security Service Headquarters in Ottawa rather than to the heads of the R.C.M.P.'s geographic divisions. Under Commissioner Simmonds, who

---

[26] *Ibid.*, paragraph 63.

[27] *Ibid.*, paragraph 306.

[28] House of Commons, *Debates*, June 20, 1969, p. 10637.

became Commissioner in 1977, the change has been somewhat in the opposite direction. Largely in response to the events that led to the appointment of this Commission, Commissioner Simmonds has taken steps to bring the supervision of Security Service practices and policies more closely under his control.

Current organization and strength of the Security Service

85. To complete this account of the evolution of the R.C.M.P. Security Service we shall provide a brief account of its internal organizational structure, the size of the Service and the distribution of members amongst its various functions and services.

86. The head of the Security Service is the Director General. The Director General reports to the Commissioner of the R.C.M.P. who, under the direction of the Minister (the Solicitor General), "has the control and management of the force and all matters connected herewith".[29] The Director General has a rank equivalent to a Deputy Commissioner, the second highest rank in the R.C.M.P. There are now four persons at this rank at Headquarters: besides the Director General, there are Deputy Commissioners for Criminal Operations, Administration and Canadian Police Services. Since 1977 an executive committee, constituted by these four and chaired by the Commissioner, advises the Commissioner on policy matters relating to all aspects of R.C.M.P. activity, including the Security Service.

87. Within the Security Service, immediately under the Director General, are three Deputy Directors General, one for Administration, one for Services and one for Operations. The Deputy Director General for Administration directs the financial and personnel administration of the Service, its training programmes and its office of internal security. Under the Deputy Director General for Services are branches which provide technical services directly to the operational branches. These branches include the Security Service's records section and automated information retrieval facility and branches responsible for physical surveillance and all aspects of electronic surveillance. The operational branches of the Security Service report to the Deputy Director General for Operations (D.D.G. Ops.).

88. Intelligence collection and countering responsibilities are assigned to three operational branches reporting to the Deputy Director General of Operations. Two of these branches concentrate on counter-intelligence activities against foreign intelligence agencies. The third of these operational branches is concerned with domestic subversion and is roughly equivalent in size to the two counter-intelligence branches combined. The only major fluctuation in these arrangements during the 1970s was the rise and fall of "G" Operations branch between 1971 and 1976. This branch focussed on 'subversive activities' related to separatism in Quebec. Its activities resulted in incidents which gave rise to this Commission and which will be fully reported upon later in our Report. "G" Operations was phased out in 1976. In addition to these investigative operational branches, there are three other branches

[29] R.S.C. 1970, ch.R-9, s.5.

which have operational roles: one is devoted to carrying out the R.C.M.P.'s security screening functions, a second specializes in the development and administration of 'human sources', and the third performs an intelligence co-ordination function.

89. There are two additional organization units directly under the Director General. The Security Service has a small audit group which we describe in some detail in Part VI of this Report. The Director General also has a secretariat which provides staff support services to him in a number of areas: co-ordinating Security Service contributions to the interdepartmental committee system exclusive of any intelligence co-ordination function; operating the yearly planning cycle; conducting policy studies; and initiating research. An organizational chart of the Security Service is annexed as Appendix "V".

90. The total establishment of the Security Service (including public service employees) actually declined as a percentage of the R.C.M.P.'s total establishment. Slightly less than half of the Security Service's staff is located at R.C.M.P. Headquarters in Ottawa. Field units are located in a number of the geographic divisions of the R.C.M.P. As was explained earlier, since the Security Service was given National Divisional Status in 1976, these field personnel report through Security Service Area Commanders to Security Service Headquarters in Ottawa.

91. Expenditures by the Security Service do not represent the full costs incurred, as the Security Service receives a number of services and forms of support (for example, accommodation in R.C.M.P. buildings, R.C.M.P. administration and pension payments) which are not billed to it directly.

C. THE R.C.M.P. SECURITY SERVICE: CURRENT ROLE

The Cabinet Directive of 1975

92. In the 1970s there was increasing concern on the part of the Security Service and the Solicitor General over the lack of a clear government mandate for the surveillance and preventive activities of the Security Service. The scope of these activities had, as we explained earlier, widened considerably in the 1960s and early 1970s. The only explicit government guidelines on security threats — the Cabinet Directives, regulations and legislation relating to security screening and internment in preparation for war — had been drawn up in the Cold War period. At that time threats to Canada's internal security were identified basically in traditional ideological terms as espionage conducted by Communist régimes, Communist groups on the far left of the ideological spectrum, and to a lesser extent, groups on the far right. But the perception of threats to security and the concept of subversion were gradually extended to encompass a wide spectrum of groups associated with radical dissent, political, social and constitutional change and the use of demonstrations and confrontations for political purposes. Security Service surveillance of these groups was not directed by any explicit government policy or guidelines. Nor was there explicit authorization for a number of the investigative and countering activities developed over the years by the R.C.M.P. in its security work.

93. The absence of clear authorization for R.C.M.P. security activities was partially alleviated on July 1, 1974, when section 16 of the Official Secrets Act came into force. This legislation[30] empowered the Solicitor General of Canada to issue a warrant authorizing the interception or seizure of communications for security purposes. The relevant parts of section 16 are as follows:

> 2. The Solicitor General of Canada may issue a warrant authorizing the interception or seizure of any communication if he is satisfied by evidence on oath that such interception or seizure is necessary for the prevention or detection of subversive activity directed against Canada or detrimental to the security of Canada or is necessary for the purpose of gathering foreign intelligence information essential to the security of Canada.
>
> 3. For the purposes of subsection (2), "subversive activity" means:
>
> (a) espionage or sabotage;
>
> (b) foreign intelligence activities directed toward gathering intelligence information relating to Canada;
>
> (c) activities directed toward accomplishing governmental change within Canada or elsewhere by force or violence or any criminal means;
>
> (d) activities by a foreign power directed toward actual or potential attack or other hostile acts against Canada; or
>
> (e) activities of a foreign terrorist group directed toward the commission of terrorist acts in or against Canada.

This section went some way towards implementing the Royal Commission on Security's recommendation for legislation authorizing the Security Service's use of certain investigative techniques. But it fell well short of providing a clear and comprehensive authorization for Security Service operations.

94. In his testimony before us the Honourable Warren Allmand explained that soon after he became Solicitor General in 1973 he came to the conclusion that the R.C.M.P. Security Service "needed a clearer and more understandable mandate", a mandate, as he put it, "that was up with the times" (Vol. 114, pp. 17536, 17543). Mr. Allmand has testified that he was seeking more than clarity. He also felt that there should be some reduction in the scope of Security Service surveillance. He told the Commission that:

> Well, what existed before was unclear, but in my mind the guidelines would make clear that certain targets which had been targets in the past should not be targets in the future... There was sometimes a tendency to consider a left wing activist group as subversive even though they did not believe in carrying out their work contrary to the law or in a violent way, and I felt that was wrong, even though we may disagree with the purpose of those groups.
>
> (Vol. 116, pp. 17917-18.)

95. Mr. Dare, the Director General of the Security Service, told the Commission that the Security Service was at that time, independently of the Solicitor General, coming to the view that a new government 'mandate' was needed. Indeed in Mr. Dare's view, "the whole of the initiative to seek a mandate came

---

[30] Protection of Privacy Act, S.C. 1973-74, ch.50.

from within the Security Service". He explained that the impetus for this initiative came from the "allegations of impropriety" associated with the Watergate affair in the United States. The need for a new mandate was confirmed at a meeting of senior field officers of the Security Service in the fall of 1974 which was addressed by Mr. Gordon Robertson, the Secretary to the Cabinet. According to Mr. Dare, Mr. Robertson told the Security Service officers that "it is quite obvious that your people are in need of clear direction" (Vol. 125, pp. 19463-65).

96. A memorandum proposing a new mandate was prepared within the Security Service, reviewed by the Solicitor General and his senior advisers and submitted by the Solicitor General to the Cabinet for final approval in March 1975. On March 27, 1975, the Cabinet approved the following guidelines for Security Service activities:

> *The Role, Tasks and Methods of the R.C.M.P. Security Service*
>
> The R.C.M.P. Security Service be authorized to maintain internal security by discerning, monitoring, investigating, deterring, preventing and countering individuals and groups in Canada when there are reasonable and probable grounds to believe that they may be engaged in or may be planning to engage in:
>
> (i) espionage or sabotage;
>
> (ii) foreign intelligence activities directed toward gathering intelligence information relating to Canada;
>
> (iii) activities directed toward accomplishing governmental change within Canada or elsewhere by force or violence or any criminal means;
>
> (iv) activities by a foreign power directed toward actual or potential attack or other hostile acts against Canada;
>
> (v) activities of a foreign or domestic group directed toward the commission of terrorist acts in or against Canada; or
>
> (vi) the use or the encouragement of the use of force, violence or any criminal means, or the creation or exploitation of civil disorder, for the purpose of accomplishing any of the activities referred to above;
>
> (b) the R.C.M.P. Security Service be required to report on its activities on an annual basis to the Cabinet Committee on Security and Intelligence;
>
> (c) the Solicitor General prepare for consideration by the Prime Minister a public statement concerning the role of the R.C.M.P. Security Service.

We will have much to say about this Security Service mandate in subsequent chapters and, indeed, in Part V we will be advancing our own proposals for what we consider to be, in form and in substance, a more appropriate authorization for security intelligence activities. In this historical overview we wish only to note the most significant features of this mandate.

97. At the outset it is important to note the legal status of the Cabinet decision with respect to the Role, Tasks and Methods of the R.C.M.P. Security

Service. This decision took the form of a Cabinet Directive. Such a directive does not become part of the *laws* of Canada. When we speak of the *laws* of Canada, in either the federal or provincial context, we mean statutes, subordinate legislation in the form of statutory instruments and the decisions of the courts in interpreting statutory provisions or in applying the common law. Cabinet Directives and Records of Cabinet decisions do not have the status of law in the sense described above. This means, among other things, that such a directive cannot be invoked as authority to do what is otherwise contrary to law. The fact that the March 1975 Cabinet Directive did not constitute a law was clearly appreciated by the head of the R.C.M.P. Security Service, Director General Dare. On May 22, 1975, Mr. Dare wrote to all of the senior officers of the Security Service explaining the purpose and meaning of the Cabinet Directive. In that letter he wrote:

> While at first glance the ingredients of our guidelines appear to be strict legal precepts, they are not.

98. The phrasing of the 1975 Cabinet Directive closely resembles a statement made by Prime Minister Trudeau in the House of Commons on July 11, 1973, concerning the criteria used to determine whether a group or an individual constitutes a security risk:

> With respect to other individuals, groups or members of groups the following criteria are applied: those engaged in or planning to engage in espionage; sabotage; foreign intelligence activity directed towards gathering intelligence information about Canada; activities directed towards creating civil disorder or accomplishing governmental change within Canada or elsewhere by force or violence or any criminal actions; or activities directed towards actual or potential attack or other hostile acts against Canada.[31]

It should also be noted that the list of authorized Security Service targets in the 1975 Cabinet Directive was built upon the definition of 'subversive activity' in section 16(3) of the Official Secrets Act. The phrase "governmental change" in the third paragraph of the mandate was rendered somewhat more ambiguous by the fact that the French version of the Directive also referred to "*un changement gouvernemental*" whereas the counterpart to this paragraph in section 16(3) of the Official Secrets Act used the words "*un changement de gouvernement*". This change would appear to broaden Security Service surveillance to cover activities involving the use of force, violence, or criminal means to change a government policy as well as to change a government. Terrorist activities of *domestic* groups were added to terrorist activities of foreign groups. Paragraph (vi) referred to a new category of activity not included in the Official Secrets Act list.

99. The addition of the sixth paragraph was quite significant. So far as the Security Service is concerned, it was clearly intended to add a good deal as the Security Service had pressed for an additional clause of this kind precisely on the grounds that it felt unduly constrained if *all* of its activities had to be confined to the limits imposed on the use of electronic surveillance by section 16 of the Official Secrets Act. Also, the Memorandum to Cabinet accompan-

---

[31] House of Commons, *Debates*, July 11, 1973, p. 5499.

ying the March 27 guidelines explained that the addition of the sixth clause meant that there need be no change in the existing range of Security Service activities. This would appear to have been the Director General's understanding of the Directive. In his letter of May 22, 1975, to senior officers of the Security Service, the Director General, Mr. Dare, emphasized that the guidelines were intentionally broad and were not intended to alter fundamentally the Security Service's current activities. The Security Service, he wrote:

> . . . will continue to monitor traditional areas of interest — such as Communists, Trotskyists, Marxists, separatists, bloc revolutionaries, native extremists, right-wing extremists and revolutionaries from other countries resident in Canada.

100. The 1975 Cabinet Directive did not specify the methods of investigation or of countering which would be employed by the Security Service. It simply indicated that the Security Service could carry out a number of activities — namely, discerning, monitoring, investigating, deterring, preventing and countering — in relation to a list of activities. Mr. Dare's letter of May 22 interpreting the Cabinet Directive emphasized that:

> *Members of the Security Service must act within the limits of the guidelines and within the limits of the law.* (The italics were his)

101. The 1975 Cabinet Directive was not publicly disclosed at the time it was agreed to. On October 28, 1977, Mr. Francis Fox, then Solicitor General, paraphrased the main terms of the Directive in the House of Commons, and it was publicly disclosed in its entirety for the first time, by us, on July 31, 1978.

Other components of the Security Service

102. The 1975 Cabinet Directive did not purport to be an exclusive and comprehensive statement of the Security Service's role. As we have related in section B of this chapter, in the years following World War II the R.C.M.P. was designated the investigative agency for security screening programmes in relation to Public Service employment, immigration, citizenship and certificates of identity. The correspondence, memoranda and Cabinet Directives establishing these programmes continue to be sources of authority for Security Service activities.

103. Here we will state only that under one or the other of these security screening programmes the Security Service might be asked to collect and report intelligence about a subject which does not fit within the list of activities in the 1975 Cabinet Directive. One example of this with respect to security screening of the Public Service is that beginning in 1965, as a result of views expressed at a meeting of a committee of senior government officials the previous year, the R.C.M.P. included in its reports information about the separatist associations of candidates for security clearances. Some confusion arose after March 1975 as to whether the Security Service should continue to provide this information. The Cabinet appeared to settle this point by deciding on May 27, 1976 that:

> information that a candidate for appointment to a sensitive position in the public service, or a person already in such a position, is a separatist or a

supporter of the Parti Québecois, is relevant to national security and is to be brought to the attention of the appropriate authorities if it is available;

However, the Cabinet did not clarify how information about separatists who were not engaging in activities listed in the 1975 Cabinet Directive should become "available" to the Security Service. The policy problems inherent in this situation will be reported upon in more detail in Part V of this Report.

104. Another government programme which has formed part of the R.C.M.P.'s security intelligence mandate concerns the preparation in advance of lists of persons to be interned under the War Measures Act in the event of a proclamation under the Act. As we indicated above, this programme was actively maintained at the peak of the Cold War and the R.C.M.P.'s contribution to it constituted one of the Force's major responsibilities in the field of security intelligence. In recent years it has been relatively dormant. We shall examine this programme in detail in Part IX of this Report and make our recommendations with regard to it.

105. In addition to formal programmes of intelligence collection discussed in the preceding paragraphs, there are many other contexts in which the R.C.M.P. Security Service is asked or expected to provide intelligence to governments and police forces for the protection of security. For instance, the Security Service is expected to provide those who are responsible for protecting international dignitaries visiting Canada with assessments of possible threats to the safety of such persons. The Security Service plays a similar role with respect to Canadian V.I.P.s, international events in Canada, and airport security. In all of these, and other contexts, the Security Service's role is not to provide the actual protection but the intelligence upon which those responsible for the protection can base their security measures. Similarly, in responding to security crises brought about by terrorist actions or other forms of political violence the Security Service's role is to provide intelligence to federal and provincial authorities responsible for dealing with the crises.

106. The Government of Canada has developed plans for responding to emergencies. The Civil Emergency Planning Order,[32] passed on June 8, 1965, requires that the Minister of Justice (now, presumably, the Solicitor General):

(2) Through the Royal Canadian Mounted Police,

(a) exercise responsibility for

(i) the internal security of Canada in all matters of subversion and espionage,

(ii) the protection of specified Vital Points;

(iii) Port and Travel Security Control;

(iv) the administration and operation of civilian internment camps, and

(v) the providing of assistance to other services and departments in the identification of persons unable to identify themselves;

(b) exercise responsibility in accordance with the police jurisdiction of the R.C.M. Police and in co-operation with other police forces, for the

[32] P.C. 1041.

internal security of Canada in all matters of sabotage and police assistance in the enforcement of federal statutes and emergency legislation; and

(c) assist provincial and municipal governments and their police forces, as requested, in all matters pertaining to the co-ordination of emergency police planning and operations.

107. Similarly the Government War Book assigns a number of functions to the R.C.M.P. in the event of war. While these emergency and wartime plans do not specifically refer to the Security Service or its predecessors, it is reasonable to infer that it would be this Service of the R.C.M.P. which would be expected to provide the security intelligence required by the R.C.M.P. to carry out the duties assigned to it in emergency and wartime situations.

D. THE R.C.M.P. "P" DIRECTORATE, FOREIGN SERVICES DIRECTORATE AND EMERGENCY RESPONSE TEAMS: CURRENT ROLES

108. During the 1970s three changes were made in the internal organization of the R.C.M.P. which relate to the Force's security responsibilities. The first was the establishment in 1973 of the Protective Policing Directorate ("P" Directorate) which grouped together in a single directorate those branches and sections of the Force involved in providing protective services for government property, personnel and information. The formation of "P" Directorate stemmed in part from the Royal Commission on Security's recommendations that all agencies concerned with protection against electronic eavesdropping

> . . . should be combined in one part of the protective security branch of the Security Service.[33]

109. "P" Directorate is not part of the Security Service. Its Director reports to the Deputy Commissioner, Criminal Operations. Most of the component parts of "P" Directorate had previously been part of the Criminal Investigation Branch. Counter-technical intrusion responsibilities constituted the only function previously performed by the Security Service. Other responsibilities assigned to "P" Directorate include airport policing, security engineering, V.I.P. protection, advice to government departments on physical security, and administration of the Canadian Human Rights Act as it applies to the R.C.M.P.

110. The emphasis in "P" Directorate is on the provision of protective services rather than investigation. Where intelligence about groups or individuals who may threaten security is required by those providing the protective service (for example, in protecting airports or visiting dignitaries), it would normally be supplied by the R.C.M.P. Security Service.

---

[33] *Report of the Royal Commission on Security*, paragraph 229.

111. The second change occurred in 1979 with the establishment of a Foreign Services Directorate to co-ordinate all R.C.M.P. foreign liaison activity. The Foreign Services Directorate brought together the Security Service and Criminal Investigation Directorate components of the R.C.M.P.'s Foreign Liaison Services under a single commanding officer who reports to the Commissioner of the R.C.M.P. through a committee of senior officers whose membership includes the Director General of the Security Service. This change affects the R.C.M.P. liaison officers who are stationed abroad at 28 Canadian missions and who, among other duties, are responsible for the security vetting of all persons applying to emigrate to Canada as permanent residents. These liaison officers, whether involved in police liaison, security liaison, or screening for visas are now members of the Foreign Services Directorate.

112. Creation of the R.C.M.P.'s Emergency Response Teams was the third change. They constitute one other component of the Force which has a role in emergency situations threatening the security of Canada. As their name implies, the function of these units is not to gather intelligence about threats to security but to respond to an emergency once it occurs. A number of municipal police forces have developed similar units. The R.C.M.P. Emergency Response Teams are now established at both the divisional and detachment level at various locations across Canada. These teams may be called upon in emergency situations such as an embassy takeover, a V.I.P. hostage-taking, an airline hijacking or a prison riot. Through courses at the Canadian Police College, the R.C.M.P also provides educational assistance to the special crisis teams of other police forces.

E. THE DEPARTMENT OF THE SOLICITOR GENERAL

113. The Government Organization Act of 1966 created the Department of the Solicitor General and transferred to it the powers, duties and functions previously exercised by the Minister of Justice and Attorney General for Canada with respect to:

(a) reformatories, prisons and penitentiaries;

(b) parole and remission; and,

(c) the Royal Canadian Mounted Police.[34]

One reason for establishing this new Department was the need to give more ministerial attention to security issues. This reason was emphasized by Prime Minister Pearson in explaining the government's intention to introduce the legislation establishing the Department of the Solicitor General:

> We hope to introduce legislation shortly which will establish, among other things, the department of the Solicitor General under a minister who will have responsibility for the R.C.M.P. and for security matters. This will be a responsibility to which he will be able to give considerable time, because this increasingly important aspect of the work of the present Department of Justice will then become the responsibility of a separate minister. The new

[34] R.S.C. 1970, ch.S-12, s.4.

minister will be able to give much closer attention to these difficult problems than has been possible in the past. A high priority function of the new department will be to examine in detail the problems of espionage and subversive activities, and to determine how best to deal with them.[35]

114. The newly created department of the Solicitor General was organized on what has been referred to as "The Swedish Ministry" concept. The Deputy Solicitor General and a small departmental secretariat were to play a limited research and policy role. They were not to manage the three agencies, the Canadian Penitentiary Service, the National Parole Board and the R.C.M.P., which constitute the operational components of the Department. The Order-in-Council[36] which transferred responsibility for the three agencies to the Solicitor General designated the Commissioner of the R.C.M.P., the Commissioner of Penitentiaries and the Chairman of the National Parole Board as deputy heads of these agencies for the purposes of the Civil Service Act. The heads of these agencies, including the Commissioner of the R.C.M.P., report directly to the Solicitor General, and not to the Deputy Solicitor General.

115. The legal framework of the Department of the Solicitor General created doubts and controversy as to the powers and role of the Deputy Solicitor General in relation to all three of the agencies under the Solicitor General, and especially in relation to the R.C.M.P. In subsequent chapters of this Report we will examine this issue in more detail and make recommendations on its resolution. But here we should note that this legal controversy about the position of the Deputy Solicitor General was one of the factors which contributed to a situation in which the Solicitor General had very little access to informed advice about policy issues arising from R.C.M.P. activities, other than from the Commissioner of the R.C.M.P. and other members of the Force. Another factor which contributed to this situation was a tradition of independence from government direction which had characterized government-police relations prior to 1966. This tradition was fortified by a loosely defined legal doctrine according to which the police as peace officers are answerable only to the law, and police operations should not be interfered with by politicians. We shall examine later the validity of this doctrine as it applies to Canada. The expectations and attitudes engendered by this doctrine affected the quality of ministerial involvement in R.C.M.P. policies with respect to both criminal investigation and security intelligence activities. A point of fundamental importance, of which we became acutely aware as we conducted our inquiry, was the absence of a clear and shared understanding by Ministers, government officials and R.C.M.P. members of the policy issues relating to police and security operations about which responsible Ministers ought to be informed and on which they should be able to give direction.

116. Since 1966, the only significant change which has taken place in the organization of the Solicitor General's Department so far as security matters are concerned is the establishment of the Security Planning and Research Group (SPARG) within the Department in 1971. The original purpose of

---

[35] House of Commons, *Debates*, March 7, 1966, p. 2296.
[36] P.C. 1965-2286.

SPARG was to assist the Solicitor General in assessing the significance of security intelligence reports received from the R.C.M.P. The Solicitor General at the time, the Honourable Jean-Pierre Goyer, likened its role to that of Crown Attorneys who assess the significance of police reports of criminal activity. He told the House of Commons that the functions of this group were as follows:

> 1. To study the nature, origin and causes of subversive and revolutionary action, its objectives and techniques as well as the measures necessary to protect Canadians from internal threats.
> 2. To compile and analyze information collected on subversive and revolutionary groups and their activities, to estimate the nature and scope of internal threats to Canadians and to plan for measures to counter these threats.
> 3. To advise me on these matters.[37]

Prior to Mr. Goyer's announcement there was much speculation in Parliament and in the media that what was being created was a parallel and civilian security service. Mr. Robin Bourne, the Assistant Deputy Solicitor General who headed the Group from its inception until 1979, testified before us as follows:

> It certainly was the perception in the public mind and in the mind of some members of Parliament, that the Government... was setting up a civilian security service...
>
> (Vol. 140, p. 21503.)

He went on: "I guess we were not very clever at explaining ourselves" (Vol. 140, pp. 21503-4). SPARG was not a civilian security service. The intention of the government in establishing the Group was as explained by Mr. Goyer in outlining its terms of reference. It was to provide the Solicitor General with information on internal threats to the security of Canada and to plan for measures to counter those threats. It was hoped to carry out this long-term research by recruiting personnel with strength in a variety of disciplines so that different perspectives could be brought to bear on the assessment of security threats reported by the R.C.M.P. Security Service.

117. There is no doubt that this Planning and Research Group did stay out of operational matters. It did not become an intelligence collection agency, and an allegation to the contrary made in the House of Commons as recently as October 1977 has been firmly rebutted by Mr. Bourne in his testimony:

> Q. Now, I am asking you those questions — I want to make it clear that I am not going to ask you questions as to whether SPARG conducted any research or did any analysis in regard to the movements with which any of them may be connected. My only question is related to the placing of agents and the using of people to conduct any form of monitoring or surveillance or investigation?
>
> A. No, sir.
>
> (Vol. 142, pp. 21811-12.)

---

[37] House of Commons, *Debates*, September 21, 1971, p. 8026.

Mr. Goyer testified to the same effect when he said:

> The Security Planning and Research Group was to advise the Minister. Therefore, it had no operational role. It had no role in investigations. It was not involved in gathering any information other than what was available to the general public...
>
> (Vol. 120, p. 18848, translation.)

We are satisfied by this testimony and our own examination of R.C.M.P. files that SPARG did not become an intelligence collection agency. Indeed, Mr. Starnes, who was Director General of the Security Service when SPARG was created, was consulted about its creation and was an enthusiastic supporter. He testified:

> Q. There was debate at the time of SPARG coming into existence, about the fact that this might be a civilian security service. What is your appreciation of that comment?
>
> A. Uninformed.
>
> Q. Did you feel at any time that this could have become a civilian security service?
>
> A. Impossible.
>
> (Vol. 124, p. 19437.)

He also told us

> ... that it would have been manifestly impossible for a group of twenty to thirty persons of the kind that had been assembled, with different backgrounds and different disciplines, to carry out an operational role. They, like me,... would not have known one end of a microphone from the other, and it is manifestly absurd, and I say that there was a lot of uninformed public debate at the time about it, which was largely of a partisan political flavour, I suspect.
>
> (Vol. 124, p. 19438.)

The frequent allegations made about SPARG, to the effect that it had an operational role, as well as a more general public suspicion of the Group's activities, prompted us to examine R.C.M.P. files on SPARG and its successors. Clearly, the Force had a major interest in knowing if another Security Service was being created. Our examination of R.C.M.P. documents revealed that the Group had no operational duties of any sort and was in no way a 'parallel' civilian Security Service. Its functions were as described by Mr. Goyer to the House of Commons in September 1971. One of those functions, SPARG's role as an assessor of R.C.M.P. security intelligence reports, did not materialize to the degree originally envisioned. In part, this was because it experienced difficulty in obtaining appropriate material from the R.C.M.P. As Mr. Bourne explained to us:

> One of the reasons that SPARG really decided... to drop our initial intention to do long-term research, was that we just could not get our hands on the information that we needed to do that job.
>
> (Vol. 140, p. 21774.)

He explained that, "...I think it would have been wrong for analysts in an outside organization to have direct access to operational files" (Vol. 140, p. 21501). In recent years the Group's major contribution to assessing the significance of R.C.M.P. reports and distributing assessments to government departments has been made through an interdepartmental committee, the Security Advisory Committee, for which the Group (or Branch as it is now called) in the Solicitor General's Department provides the Chairman and support staff. We shall examine this arrangement further in section G below.

118. In December 1972, the role of the Group was expanded to include certain responsibilities for crime prevention and law enforcement matters. This change was reflected in the Group's name which became Police and Security Planning and Analysis Group. The Group was to review and analyze criminal activities, trends and developments and formulate proposals for legislative policy concerning criminal investigations and police procedures. In 1974 the Group's title was changed again, this time to Police and Security Planning Branch (P.S.P.B.). By this time it had also taken on the primary responsibility for research and development in relation to the government's capacity to respond to civil emergencies and natural disasters. The rise of terrorism as a global phenomenon, together with the need for a co-ordinated government response to natural disasters and accidents, gave increasing importance to this role.

119. The Branch, now called the Police and Security Branch (P.S.B.), is responsible for analyzing and proposing measures in response to:

- threats to the internal security of Canada from organizations, groups and individuals either in Canada or elsewhere;
- policy formulation for the protection of personnel, property and equipment in the federal government, including the security of government information;
- the role of the federal government in law enforcement in Canada; and
- contingency planning for Ministry crisis handling in emergency situations.

The Branch has three divisions which cover the functions just outlined: Security Information Analysis and Contingency Planning; Police and Law Enforcement; and Security Policy.

120. In 1973 the Cabinet established a 'lead Ministry' system under which Ministers were assigned the responsibility for co-ordinating the government's response to different types of emergency. For internal security crises, including situations ranging all the way from isolated terrorist attacks to large scale insurrection, the Solicitor General is designated as the lead Minister. In the event of such an emergency, a Crisis Centre in the Solicitor General's Police and Security Branch comes into operation.

F. THE ROLE OF OTHER DEPARTMENTS IN SECURITY AND INTELLIGENCE

121. While the R.C.M.P. Security Service has the primary responsibility for security intelligence, there are other departments of the federal government

which have responsibilities in relation to security and intelligence. An examination of the security and intelligence activities of these other federal departments is not within our terms of reference. Nonetheless, we think a brief outline will fit the role of the R.C.M.P. Security Service into the total context of the federal government's security and intelligence arrangements.

122. All of the departments and agencies of the federal government have Security Officers. These Departmental Security Officers are responsible for the physical security of departmental premises, property and communications. They also have responsibilities with respect to personnel security. Decisions as to whether a person should be granted a security clearance are made by the Deputy Minister of each Department on the basis of information given to the Department by an individual applicant and information supplied by the R.C.M.P. Security Service. Departmental Security Officers co-ordinate this security clearance process within each department.

123. A number of departments have special security and intelligence functions in addition to the physical and personnel security functions which are carried out by all departments and agencies of the federal government. We shall briefly describe these more specialized security and intelligence activities below. The organizations in the federal government which perform these activities, together with the R.C.M.P., form what is sometimes referred to as the "security and intelligence community". We now turn to a consideration of those organizations. They are: the Department of External Affairs, the Department of National Defence, the Communications Security Establishment, the Department of Supply and Services and the Canada Employment and Immigration Commmission.

The Department of External Affairs

124. The security and intelligence responsibility of the Department of External Affairs is carried out by three components of that Department: (a) the Security Division and (b) the Intelligence Analysis Division (which together make up the Bureau of Intelligence Analysis and Security), and (c) the Bureau of Economic Intelligence. A Deputy Under-Secretary of State (Security and Intelligence) directs the work of these three units.

125. The Security Division of the Department of External Affairs has responsibilities which are closely related to the R.C.M.P. Security Service. Its responsibilities with respect to personnel and physical security, especially in Canadian missions abroad, have a very important bearing upon Canada's counter-espionage capacity. Foreign intelligence agencies have attempted to penetrate the Canadian government by compromising its personnel posted abroad and gaining access to communications emanating from Canadian missions.

126. The National Security section of the Security Division has the most extensive links with the R.C.M.P. Security Service. One of its functions concerns the activities of foreign diplomats in Canada who are suspected of engaging in unacceptable intelligence activities. Such cases sometimes lead to decisions by the Canadian Government to declare a diplomat *persona non*

grata and to expel him from Canada. In these situations, the case against a diplomat is based primarily on information gathered by the R.C.M.P. Security Service and reviewed jointly by that agency and the National Security section. Close co-operation is needed to ensure that the diplomatic consequences of expulsion are balanced against the threat to Canada's security if the suspected diplomat remains in Canada. The National Security section also has responsibilities with respect to the granting of visas to foreign diplomats. The decision to grant or deny a diplomatic visa will have an important effect on the extent to which foreign intelligence officers in the guise of diplomats are admitted to Canada. The National Security section works closely with the R.C.M.P. Security Service in reviewing these applications. The Security Service is asked to provide information as to an applicant's previous involvement in intelligence activities during previous postings.

127. The Intelligence Analysis Division's principal function is to maintain a compendium of information on various geographic areas of the world based on information from the regional desks of the Department and from allied countries. The information received concerns political, economic and social trends and has been collected overtly, that is from open sources. Some of the information may relate to political developments abroad which affect the internal security of Canada. This Division does not prepare assessments of intelligence reports. Some of the information it assembles is distributed to interested government departments and agencies (including the R.C.M.P.) and to the Intelligence Advisory Committee. That committee (whose function will be described in section G below) combines reports received from various departments and agencies of the federal government, makes assessments of these reports and distributes these assessments to interested departments and agencies.

128. The Bureau of Economic Intelligence in External Affairs is responsible for the collation, storage and reporting of economic intelligence. It carries out basic assessments relevant to the intelligence priorities of 'economic' departments and agencies such as Finance, Industry, Trade and Commerce, Energy, Mines and Resources, and the Bank of Canada. These priorities are established by an Economic Intelligence subcommittee of the Intelligence Advisory Committee.

129. There is one further intelligence activity in the Department of External Affairs related to security. That is the work of the Co-ordinator for Emergency Preparedness who reports to the Director General of the Bureau of Intelligence Analysis and Security of the Department. This officer is responsible for preparing plans to deal with terrorist attacks on Canadian missions or Canadian citizens abroad. This responsibility stems from the fact that under the Government's emergency measures organization, the Department of External Affairs is the 'lead ministry' (i.e. the Department responsible for co-ordinating the government response) in the event of such emergencies occurring outside Canada. To fulfill his responsibilities the Co-ordinator uses information from open sources and overseas missions as well as intelligence reports from the R.C.M.P. Security Service.

The Department of National Defence

130. While this department has an obvious responsibility for the security of Canada in terms of the protection of Canadian sovereignty and contributing to the maintenance of world peace, it also has a number of functions which relate to the internal security of Canada and to intelligence. The security and intelligence components of the Department report to the Director General of Security and Intelligence.

131. In the area of security clearances, under the provisions of Cabinet Directive 35, the Department of National Defence conducts its own security clearance programme. While it uses its own Special Investigation Unit to conduct inquiries on the personal reliability of applicants for positions in the Canadian Armed Forces, it relies heavily on the R.C.M.P. for information about the criminal record of applicants or their participation in 'subversive' activities. In the area of technical security, the Department of National Defence, with the R.C.M.P. and the Department of External Affairs, maintains teams for the inspection of premises to detect eavesdropping devices or unacceptable audio emissions both within their own departments and agencies, and elsewhere in government. The Department of National Defence also has contact with the Departments of Supply and Services, External Affairs, and Industry, Trade and Commerce in such areas as the control of visits to and from National Defence establishments and firms employed on classified contracts, the release of classified information, the export of military equipment to foreign countries, and patent applications on military equipment.

132. With regard to intelligence, the Department of National Defence requires domestic security intelligence to fulfill its role in maintaining internal security. The phrase "internal security" as used by the Department refers to the role of the Canadian Armed Forces in support of the civil authority and can be distinguished from the fundamental *raison d'être* of the Canadian Armed Forces in the defence of Canada from foreign military aggression. Examples of internal security operations include: operations in aid of the civil power under section 235 of the National Defence Act[38] when a civil disorder or disturbance reaches a magnitude where the attorney general of a province may request the Chief of the Defence Staff to provide troops; armed assistance to another federal department, such as the provision of troops to a federal penitentiary in response to a request from the Solicitor General; and security precautions at Department of National Defence installations directly or indirectly threatened by a civil disturbance in their vicinity.

133. All units of the Canadian Armed Forces are required to investigate minor security infractions or incidents. Actual or suspected security incidents, particularly where espionage, subversion, sabotage or arson is a possibility, are investigated by the Department's Special Investigation Unit and, if there is evidence to suggest that any of these acts have been committed, the R.C.M.P. is informed. The Special Investigation Unit also maintains a Police and Security Liaison Programme under which it combines information obtained

[38] R.S.C. 1970, ch.N-4.

from the R.C.M.P. and other police forces with information from open sources to provide intelligence on possible threats to military installations or personnel. The Special Investigations Unit does not have a mandate to collect intelligence about such threats by covert means.

The Communications Security Establishment (C.S.E.)

134. This organization is a separately organized establishment under the general management and direction of the Minister of National Defence. The Chief of C.S.E. reports to the Minister through the Deputy Minister and the Chief of the Defence Staff. One function of the Communications Security Establishment is to manage and direct a communications security programme. Policy control of this programme comes through the Interdepartmental Committee on Security and Intelligence under the general direction of the Cabinet Committee on Security and Intelligence. (A description of these committees is set out in section G below.) The object of the communications security programme is to deny to foreign powers any valuable national information which they might acquire by exploiting Canadian governmental communications. Work in this area includes providing cryptographic advice on the security of coded communications.

The Department of Supply and Services

135. This Department's responsibilities with respect to physical and personnel security are especially important in the field of industrial security. The Department's programme of industrial security is concerned with the protection of classified and sensitive information in the hands of Canadian companies undertaking work on behalf of the Canadian or other governments. The programme is intended to meet the Canadian government's national and international industrial security commitments. This programme includes responsibility for the security clearance of personnel under Cabinet Directive 35. In carrying out its responsibilities for industrial security, the Department depends on reports of security threats from the R.C.M.P. Security Service. The Industrial Security Division is sub-divided into a number of functional areas: information security; personnel security clearance; electronic data processing (E.D.P.) security; training; and field and industrial security officers. The Protective Security Division is concerned with hardware security and closed circuit television (C.C.T.V.) systems in new buildings, and with surveys of regional supply centres and printing units. The Department also has an Emergency Supply Planning Division which is concerned with the establishment of a war supplies agency in the event of war, the development of emergency supply plans to support national emergencies, the management of the government-sponsored stockpile of supplies, and with the development of an industrial preparedness programme.

Canada Employment and Immigration Commission

136. Within the Enforcement Branch of this department is the Intelligence Division. This Division is concerned chiefly with analyzing and reporting on the long-term trends in illegal immigration and in collecting and analyzing information on immigrants active in organized crime. The Division receives infor-

mation from Canadian and American police and security forces through formal and informal channels and, in co-operation with the R.C.M.P., assesses it as a prelude to expulsion or to changing the immigrant's status.

137. Within the Foreign Branch, the Security Review Division looks at applicants for entry to Canada from the security point of view. The review involves liaison between local police and security forces and the R.C.M.P. Security Service here. This process is applied in the case of information on some categories of visitors, on suspected or known terrorists who may be coming to Canada, suspected or known intelligence officers and 'subversive' or 'front' organizations of which immigrants may be members.

G. THE ROLE OF THE CABINET AND INTERDEPARTMENTAL COMMITTEES

Background

138. Since the end of the Second World War, interdepartmental committees composed of senior civil servants have been the main centres for developing and monitoring policy in relation to security and intelligence. With regard to security policy, the most active body was the Security Panel. This committee was made up of senior officials and formed under the auspices of the Privy Council Office in 1946. It was chaired by the Secretary to the Cabinet. Initially its membership consisted of the Directors of Intelligence of the three military services, the Director General of the Defence Research Board, and representatives from the Department of External Affairs and the R.C.M.P. Later on, the membership of the Committee was expanded to reflect the broader concerns of the security community: the Department of Manpower and Immigration, Supply and Services, the Solicitor General (from 1966), and the Public Service Commission. In this later period, military representation was provided by the Deputy Minister of National Defence and the Chief of the Defence Staff. After 1953, all representatives on the Security Panel were of deputy minister rank, or its equivalent. The Commissioner represented the R.C.M.P. In 1953, in addition to the Security Panel, there was formed a Security Sub-Panel made up of officials from the same departments as were represented on the senior committee, but who were of lower rank. This body was chaired by an official in the Privy Council Office. The Security Sub-Panel carried out much of the preparatory work in formulating policy proposals for the Security Panel.

139. The main function of the Security Panel was to formulate security policy for the approval of Cabinet. The security issues with which it was primarily concerned related to physical and personnel security in government departments. For example, the Security Panel developed the security screening policies which were incorporated in Cabinet Directives after 1946. It also assumed some responsibility for the interpretation and application of government security policies. The 1963 Cabinet Directive on Security Clearance gave the Security Panel a formal part in the security screening process by requiring that the Secretariat of the Panel review all cases in which a department was

proposing to deny an employee a security clearance. Aside from security screening policies, the Security Panel had relatively little direct impact on the security intelligence collection activities of the R.C.M.P. One important exception was in relation to the collection of intelligence about Quebec separatism. In the summer of 1967, the Security Panel encouraged the R.C.M.P. to make a much greater effort to keep the government informed about the separatist movement in Quebec — its democratic and constitutional manifestations as well as its terrorist manifestations, and its connection with foreign interference activities.

140. On the intelligence side of security and intelligence affairs, the Joint Intelligence Committee, that had been established in 1942, continued after the war, until 1972 when it became the Intelligence Advisory Committee. Its function was to collate current intelligence gathered, to a large extent, from allied countries so as to alert relevant departments and agencies of government to international developments. Given the essentially international character of the intelligence procured through this Committee, it had little to do with the domestic intelligence gathering activities of the R.C.M.P. In 1960, an additional body, the Intelligence Policy Committee, was formed with membership of the deputy ministers from National Defence, Finance and Communications (after 1967), the Chairman of the Defence Research Board, the Commissioner of the R.C.M.P. and the Secretary to the Cabinet. It was chaired by the Under-Secretary of State for External Affairs. The Committee exercised general policy direction of the Canadian intelligence programme.

141. Until 1963 the Intelligence Policy Committee reported to the Defence Committee of the Cabinet, while Security Panel proposals went directly to the full Cabinet. In 1963, a Cabinet Committee on Security and Intelligence was formed to consider policy proposals brought forward by the Security Panel and the Intelligence Policy Committee. This Cabinet Committee has always been chaired by the Prime Minister. One of the Committee's first acts was approval of the revised security screening policy in the form of Cabinet Directive 35. It met only once more before the end of 1965 but was active between 1968 and the end of 1970 when it was concerned, first with the report of the Royal Commission of Security and, later, with the October crisis of 1970.

142. Until 1975, the Cabinet Committee on Security and Intelligence did not concern itself with defining the scope of Security Service surveillance. The only aspect of security intelligence targetting on which it appears to have given direction to the R.C.M.P. was with regard to Quebec separatism. In this field it urged the intensification of effort in the same direction as that advocated by the Security Panel and, at a meeting on December 19, 1969, agreed that the R.C.M.P. should be asked to provide a detailed report on the state of separatism in Quebec in terms of organizational relationships, numbers involved, strategies, tactics and foreign influence. No distinction was made between separatist groups employing legal means of advocacy and organization and those suspected of using illegal means.

143. The Royal Commission on Security recommended, *inter alia*, that a "formalized" Security Secretariat be established in the Privy Council Office to

formulate security policy and procedures and "with effective authority" to supervise their implementation. The Secretariat was to be concerned with programmes concerning physical and personnel security, and, significantly, it was to

> ... provide the link between the investigative and operational security service and government departments, and between this service and the public.[39]

In implementing this recommendation the government encountered some difficulty in determining the appropriate division of responsibilities between the Security Secretariat in the Privy Council Office and the Solicitor General who, it will be recalled, had been given a major responsibility for security policy in 1966. This question was not clearly resolved. A large security secretariat with responsibility for all major aspects of security policy was not created. A small secretariat, consisting of an Assistant Secretary to the Cabinet and one assistant, continued to deal with the security policy activity generated by the interdepartmental committee system. At the same time the capacity of the Secretariat of the Solicitor General's Department to assist with security policy matters was, as we have seen, strengthened by the establishment in 1971 of the Security Planning and Analysis Research Group.

The reorganization of the committee system

144. A major change in the interdepartmental committee system occurred in 1972 when the Security Panel and the Intelligence Policy Committee were combined to form the Interdepartmental Committee on Security and Intelligence (I.C.S.I.). The reason for merging these committees was recognition of the close relationship between external intelligence and domestic security, especially in an era of international terrorism and increasing activity by foreign intelligence agencies. Like its predecessors, this Committee's membership was at the deputy minister level. Both the Deputy Solicitor General and the Commissioner of the R.C.M.P. were members. This committee, under the general direction of the Cabinet Committee on Security and Intelligence, was to keep under review Canadian security and intelligence organization and activities. However, procedures were not established for regularly reviewing the activities of the R.C.M.P. Security Service. At first I.C.S.I. was chaired by Mr. Gordon Robertson, who was then Secretary to the Cabinet and later Secretary to the Cabinet for Federal/Provincial Relations. Successive Secretaries to the Cabinet have assumed the chairmanship.

145. Under I.C.S.I. two new committees were created — the Security Advisory Committee (S.A.C.) and the Intelligence Advisory Committee (I.A.C.). Of these the Security Advisory Committee has had the closest links with the R.C.M.P. Security Service. S.A.C. became in effect a principal bridge between the Security Service and government. The Chairman of S.A.C. until 1979 was Mr. Bourne in his capacity as Assistant Deputy Minister for Police and Security matters in the Department of the Solicitor General. His successor as Assistant Deputy Minister, Mr. Michael Shoemaker, also assumed the

[39] *Report of the Royal Commission on Security*, 1969, paragraph 46.

chairmanship. The Director General of the Security Service is the Vice-Chairman. Its membership includes the heads of the intelligence and the security branches of other government departments, namely External Affairs, National Defence, Supply and Services, Employment and Immigration, and the Assistant Secretary to the Cabinet for Security and Intelligence. The support staff for S.A.C. has come principally from the Police and Security Branch in the Solicitor General's Department.

146. S.A.C. has had two principal functions. First, it has been responsible for reviewing the adequacy of policies concerning personnel and physical security in government departments and bringing forward proposals for new policies. The responsibility concerns what might be referred to as the 'nuts and bolts' issues of government security policy. A network of sub-committees and working groups operates under the aegis of S.A.C. to deal with specialized aspects of security such as communications and computer security, the protection of nuclear materials and crisis management. S.A.C.'s second responsibility is related to security intelligence: it is to produce assessments of the internal security situation in Canada for the I.C.S.I. and the Cabinet Committee on Security and Intelligence. These assessments are based primarily on information reported by the R.C.M.P. Security Service. For a number of years such threat assessments were produced on a quarterly basis, but since 1976 these have been replaced by short weekly security intelligence reports on current domestic security developments. These reports are written by an interdepartmental drafting group attached to S.A.C., relying almost exclusively on Security Service information. Aside from security clearance reports, which are sent directly from the Security Service to government departments, S.A.C.'s weekly security intelligence reports provide the main opportunity for Ministers (other than the Solicitor General) to see security intelligence products emanating from the R.C.M.P.

147. The Intelligence Advisory Committee's sphere of responsibility is in the area of external intelligence. (One of the linguistic quirks of the intelligence community in both Canada and abroad is that at the level of government co-ordination and direction, 'intelligence' usually refers to intelligence about foreign rather than domestic matters (see footnote 8)). In contrast to S.A.C., I.A.C.'s role is primarily the collation and dissemination of external intelligence and the preparation of periodic intelligence assessments. It is chaired by the Deputy Under-Secretary of State (Security and Intelligence), for External Affairs. Its membership includes the Director General of the Security Service and the heads of branches of other departments with responsibilities in the field of external intelligence. One of I.A.C.'s sub-committees is responsible for identifying intelligence requirements and priorities, but this identification of intelligence priorities has had very little impact on the activities of the R.C.M.P. Security Service. I.A.C. has a small support staff, consisting of three seconded officers and a committee secretary, in the Privy Council Office. Through interdepartmental drafting groups and with the help of the seconded staff, I.A.C. produces special and general assessments of particular subjects as well as a weekly collation of external intelligence. The R.C.M.P. Security Service contributes to both kinds of product, but given the domestic focus of its work, its contributions have not been a major component of I.A.C. reports.

148. The Cabinet Committee on Security and Intelligence continued through the 1970s to preside at the apex of the interdepartmental committee system. Its most important contribution to the direction of the R.C.M.P. Security Service was its approval in March 1975 of a new mandate for the Security Service. That decision called for an annual Report to the Cabinet Committee of the Security Service's activities. (Before that, in the 1970s, there had been three audio-visual presentations by the Security Service to the Committee providing a very general overview of its work.) Since 1975 the Security Service has submitted only two 'annual' reports to the Cabinet Committee describing its main achievements and difficulties.

PART III

PROBLEMS IN THE SYSTEM: R.C.M.P. PRACTICES AND ACTIVITIES "NOT AUTHORIZED OR PROVIDED FOR BY LAW". INSTITUTIONALIZED WRONGDOING

INTRODUCTION

CHAPTER 1: Improper Acts

CHAPTER 2: Surreptitious Entries: Security Service and C.I.B.

CHAPTER 3: Electronic Surveillance: Security Service and C.I.B.

CHAPTER 4: Mail Check Operations: Security Service and C.I.B.

CHAPTER 5: Access to and Use of Confidential Information — C.I.B.

CHAPTER 6: Access to and Use of Confidential Information — Security Service

CHAPTER 7: Countering: Security Service

CHAPTER 8: Physical Surveillance

CHAPTER 9: Undercover Operatives

CHAPTER 10: Interrogation of Suspects

CHAPTER 11: Acts Beyond the Mandate

INTRODUCTION

1. In this and the next three parts we express a number of serious concerns about the ability of the Security Service, both in recent years and in the future, to perform adequately and effectively those functions which we think are appropriate for Canada's security intelligence agency. Before we explain our concerns, however, we think it fair to observe that the many dedicated men and women in the Security Service are far from having failed on all fronts. Indeed, putting it positively, they have had successes. Success is not measured easily in security intelligence work: it is not always clean cut and only rarely known to the public. The public learns of successes when for instance, a defector from the intelligence service of a foreign country, such as Igor Gouzenko, brings positive evidence of espionage, so that charges can be laid under the Official Secrets Act and any foreign diplomats involved can be declared *personae non gratae*. Such an expulsion of diplomats is often the public's signal of a success of the Security Service. In 1978, thirteen members of the Soviet mission were declared *personae non gratae* after they attempted to develop a member of the R.C.M.P. Security Service as an agent. Between 1976 and 1980, four members of Soviet military intelligence have been either declared *personae non gratae*, or not had their visas renewed as a result of their efforts to develop agents in Canada who had access to classified technical information. Another publicly known 'success' led to the expulsion of members of the Cuban mission in 1977. As a result of our inquiry the public has become aware of the detection and apprehension in 1976 of a visitor to Canada who was a member of the Japanese Red Army. The detection of the use of Mr. George Victor Spencer by the Soviets became public in 1966.[1] We have made public the essential details of an operation in which agents of a foreign intelligence service were detected and their activities frustrated (Vol. 315, pp. 301402-12). The trial of Mr. Bower Edward Featherstone in 1967 resulted in his conviction on a charge of espionage.[2]

2. Those are among the successes of the Security Service that are publicly known and officially acknowledged. From time to time other successes attributed to the Security Service by the media have been neither confirmed nor denied.[3] Others have not been publicized for operational or diplomatic reasons. Foreign diplomats whose activities as agents have been established are not always asked to leave Canada; sometimes their visas are allowed to expire, or the Department of External Affairs advises their ambassador that their return from home leave would not be welcomed. In such cases there is no official publicity and frequently the matter is not discovered by the media.

---

[1] *Report of the Commission of Inquiry into Complaints made by George Victor Spencer*. Ottawa, 1966.

[2] Referred to in our First Report, *Security and Information*, paras. 10 and 12.

[3] e.g., Articles in the *Toronto Sun*, August 24 and August 25, 1980, reporting claims by a Canadian citizen who had immigrated from the U.S.S.R. that he had been an illegal agent of the K.G.B. and had been detected by the Security Service.

3. In some areas of counter-espionage and the detection of unacceptable foreign interference in Canadian affairs the Security Service has been more effective than in others because their personnel involved in those areas have been less severely hampered by constant transfers.

4. In some investigations of leaks of classified government documents the Security Service have identified the source without being able to collect enough evidence to obtain a conviction, and steps have been taken to prevent the suspect from doing further damage. The Security Service's role in the security screening programme, which we report on in Part VII, would appear to have at least been partially successful in ensuring that classified information and classified installations of the federal government are protected. The Security Service, by the collection of intelligence, has contributed significantly to the programme that involves "P" Directorate of the R.C.M.P., local detachments of the R.C.M.P. and other police forces in the protection of visiting foreign dignitaries and Canadian public figures who are open to physical attack. We must mention the work of the Security Service in planning and carrying out security arrangements for the Olympic Games in Montreal in 1976, the Habitat Conference in Vancouver in 1977, and the Commonwealth Games in Edmonton in 1978, all of which had the potential for terrorist acts of the kind seen at Munich in 1972.

5. This is an impressive list. It reflects the investigative skills of well-trained policemen — skills which we think the Canadian security intelligence agency should be able to continue to include in its arsenal. Nevertheless, in this Part, we shall demonstrate the breakdown of the rule of law in the Security Service, and in Part V show the deficiencies in the Security Service and in the R.C.M.P. itself that reduce the effectiveness of the Security Service. We shall also describe the failures in the R.C.M.P. to appreciate and accept the proper relationship between the civilian authority (the government) and a police force or security intelligence agency. There is of course no way in which all these deficiencies can be established as having caused failures in *particular* cases of counter-espionage operations, counter-subversion activities, security screening or the protection of V.I.P.s. Often a failure is not easy to detect, or to prove conclusively; when it is, it is not always possible to pinpoint the organizational deficiency (if there was one) that caused it.

6. The most we can do is point to the deficiencies and balance them against the successes. Our conclusion will be that to ensure the level of effectiveness which Canada is entitled to expect of a security service, respect for the law, acceptance of civilian authority, and respect for the liberties of the individual, significant changes are necessary in the present philosophy and structure of the security intelligence agency, and of the methods by which it accounts to government and Parliament and is controlled by government.

7. In Part II we described the evolution of the system developed for responding to security threats. In this Part we turn to what might be described as a breakdown in the system. Here we shall report on the history and development of a number of investigative practices used by the R.C.M.P. in both criminal investigations and the work of the Security Service. Where we speak of the

"C.I.B." we refer to the Criminal Investigation Branch, now known officially as "C" Directorate.

8. As we examine these investigative practices we shall analyze whether their use has constituted conduct "not authorized or provided for by law" — whether the criminal law, some other federal or provincial statute that creates an offence or contains a prohibition, or the civil law enforceable by actions in the courts for damages, declaratory judgments or injunctions. This analysis is as comprehensive as we have been able to make it. We have considered not only those issues that have attracted considerable public attention but many that have gone relatively unnoticed. Given our commitment to the principle that both our national police force and the security intelligence agency should operate within the law, we have considered it our duty to analyze and make recommendations about all legal issues that have come to our attention in regard to investigation methods and other methods of carrying out duties. Many of these are issues which the R.C.M.P. itself has asked us to consider; others have been raised by ourselves.

9. This part of our Report will contain a reasonably detailed summary of the history of each practice and the development of the policies concerning it. This is an essential preliminary, first to the analysis of the legal issues that is found in this Part, and second to our recommendations for legislative reform found in Part V, Chapter 4 (as to the security intelligence agency) and in Part X, Chapter 5 (as to criminal investigations by the R.C.M.P.). They are also important as background to matters that will be reported on in our Third Report, which will, among other things, consider the extent to which senior members of the R.C.M.P., Cabinet ministers and public officials have been aware of those practices that are contrary to law.

10. Some of what is said in this Part as to the extent and prevalence of each practice will also form the foundation for our observations as to the need for each of the practices that has given rise to legal problems. Those observations are found in Parts V and X as a preliminary to our recommendations for legislative reform.

11. In some of the chapters of this Part the analysis of the legal issues will be thought lengthy by some readers. We make no apology. We believe that the R.C.M.P., the government and the public are entitled to have not only our conclusions as to lawfulness but also the reasons for our conclusions. Moreover, at times our conclusions are different from those that have been expressed by agencies of government, and we think that if we are going to differ we should say why.

12. In addition to practices that were contrary to law, there were activities that, while not contrary to law, were nevertheless "not authorized. . . by law" in the sense that they cannot be said to have been within the authority given to the R.C.M.P. by the R.C.M.P. Act or by regulations or ministerial directives made under that Act. It is that category of activities which we examine first.

CHAPTER 1

IMPROPER ACTS

13. We propose to discuss here a topic which is of the utmost importance but which is very difficult to examine at length without reference to specific incidents. The specific incidents on which we base our general conclusions here will be described in detail in a later Report. For reasons which we shall mention shortly we consider that it would not be proper to set out those incidents in this Report.

14. In Part I, we outlined the interpretation we have placed on our terms of reference. We pointed out that we have not considered that, in examining conduct of members of the R.C.M.P., we were restricted to looking at activities "not authorized or provided for by law". We indicated in our opening statement on December 6, 1977, that it was our intention to look at the moral and ethical implications of the conduct of members of the Force.

15. The general standards of conduct for the R.C.M.P. are explicitly laid down in section 25(o) of the R.C.M.P. Act which makes it a major service offence if a member

> (o) conducts himself in a scandalous, infamous, disgraceful, profane or immoral manner.

During the course of our examination of the R.C.M.P. and its Security Service a number of incidents have come to our attention which in our opinion constitute improper conduct and which we consider form enough of a pattern to be considered "institutionalized". Because each of them discloses conduct on the part of members which may constitute a major service offence under the R.C.M.P. Act, we do not propose to discuss details of the incidents in this Report. They will be dealt with in the Report which covers other incidents involving specific members whose conduct may have been illegal.

16. The common thread which we have detected running through these incidents is that of a willingness on the part of members of the R.C.M.P. to deceive those outside the Force who have some sort of constitutional authority or jurisdiction over them or their activities. We have come to this conclusion reluctantly and regretfully because in our view it might well be the most serious charge which we are levelling against the Force in our Report. Nevertheless, we are convinced that the practice existed. We have received evidence that federal Ministers of the Crown responsible for the R.C.M.P. were misled by the R.C.M.P. and that on other occasions relevant or significant information was intentionally withheld from Ministers. There is evidence that the same thing has occurred at the provincial level with respect to a provincial minister. There is also evidence that there was a similar approach adopted by the Force in dealing with senior public servants. The extent to

which such matters are established and form part of a widespread attitude by the Force that it need not be responsible to civilian authority will be looked at in Part X.

17. The purpose of this practice of deception does not appear to be to protect any particular member or members who might have been involved in some unlawful or improper conduct. Rather, it is based on one or the other of two misguided notions. One such notion is that the Minister responsible for the R.C.M.P. should not be fully informed of a questionable activity by the Force so that, if asked, the Minister can deny any knowledge about it. To inform him would, according to this notion, put him in an untenable position. Such a strategy should not be confused with the notion of "plausible deniability", a concept used in the United States to describe an "aversion to making written records of presidential authorization of sensitive intelligence-related operations.[1] The practice we are referring to did not involve avoidance of written evidence of high level approval but a decision not to inform Ministers of operations and policies which it would be difficult for a Minister to justify if questioned in the House of Commons. Each Solicitor General who appeared before us stated emphatically that he did not accept, as a norm to be applied to the accountability of the R.C.M.P. to the responsible Minister, the proposition that the Minister should not be informed of unlawful or even questionable acts. We agree wholeheartedly that withholding such information is unacceptable, even though there may be circumstances where the result of candour is extremely difficult and embarrassing for the Minister.

18. The other notion which has given rise to the practice of deception is that exposure to the Minister, and then perhaps publicly, of any questionable activity on the part of its members would inflict damage to the good reputation of the Force and that this concern is of greater weight than any need for candour, truth and forthrightness. This notion arises in part from the fact that the Force has become a national symbol, probably more so than any other Canadian institution or object. Protecting the Force's reputation is also a manifestation of a broader problem, which we will examine in Part VI, related to the unquestioning loyalty to the Force engendered in its members. We there point out that the R.C.M.P., through its recruiting, training and management practices, engulfs its members in an ethos akin to that found in a monastery or religious order. Extreme loyalty, untempered by an awareness that, among other things, the Force has a duty to be candid and forthright with the civilian authority, has contributed to both the practice of deception and an unwillingness, on the part of members not a party to a deception but aware of it, to disclose the deception to the Minister.

---

[1] *Report of Department of Justice Concerning Its Investigation and Prosecutorial Decisions with respect to Central Intelligence Agency Mail Opening Activities in the United States*, Department of Justice, Washington, Jan. 14, 1977, p. 11.

CHAPTER 2

SURREPTITIOUS ENTRIES — SECURITY SERVICE AND C.I.B.

INTRODUCTION

1. The practice by police forces of secretly entering premises, in the course of an investigation, without the consent of a person entitled to give consent is a serious intrusion into civil liberties, and deserves a detailed scrutiny. The need for such a practice, the implications of the search and handling of private property and possessions and the installation of devices for intercepting private communications, and above all, the assumptions of police forces as to their rights under the law, are the focus of discussion in this chapter. The practices of the two arms of the R.C.M.P., the C.I.B. and the Security Service, are examined separately, since the purpose of and policies relating to surreptitious entry by each of them are somewhat different. What is the same in both cases is the overriding misapprehension of the R.C.M.P. about the lawfulness of this practice, and for this reason we detail some of the areas of the law under which policemen might be liable to be charged as a result of this investigative practice.

A. NATURE AND PURPOSE OF THE PRACTICE: SECURITY SERVICE AND C.I.B.

The nature of the practice

2. We use the phrase "surreptitious entries" to describe entries into premises to which the public does not have access, without a search warrant or other lawful authority, and without the consent of the person who has the right in law to give or refuse it. Surreptitious entries are often made to survey premises in preparation for the installation of an electronic listening device, and then for the installation, monitoring, repairing and removal of the device, or to search premises, examine what is found there, and copy or photograph objects or documents. Sometimes objects or documents have been removed from the premises to be photographed and returned as soon as possible. Sometimes objects or documents thus removed have not been returned; sometimes they have been destroyed. In all these situations of surreptitious entry a common element is that the R.C.M.P., whether in the work of criminal investigation or of security, intend that the person whose premises are under investigation should not become aware of the operation, either at the time or later.

Consequently, the investigators are careful not to leave any evidence of their having been present.

3. Most of the formal policy developed by the R.C.M.P. concerning surreptitious entries and, accordingly, most of the evidence before us, relates to technical installations intended to intercept communications from, to, or among suspects, either by wiretaps or microphones. Many, but not all, of these installations require surreptitious entry to premises occupied or about to be occupied by the suspects. Sometimes entry is not needed, either because of the nature of the target or the technique employed. On other occasions installations can be completed with the consent of the owner or occupier of premises, either before or during a period of temporary occupancy by the suspect.

4. Some technical aspects of possible legal interest in the consideration of this subject should be mentioned. The installation of microphones or wiretaps does not, for obvious reasons, involve any substantial damage to the structure of a building, but on some occasions temporary physical damage is caused, and then is patched and disguised. In addition, while most installations supply their own power from batteries, on occasion a minor amount of electric power may be obtained from the supply on the premises, past the meter, as has been disclosed publicly on occasion in the trials of criminal cases.

5. It is certain that the development of the sophisticated skills necessary for surreptitious introduction of technical devices has led to an increase in the use of surreptitious entries over the past 20 years. However, the evidence is clear that surreptitious entry by members of the R.C.M.P. to secure intelligence concerning criminal activities, or activities of special interest to the Security Service, preceded the development of the techniques for electronic surveillance. The evidence before us indicates clearly that before the widespread use of electronic surveillance both the C.I.B. and the Security Service employed such entries to observe and photograph objects and documents. In addition to obtaining information and photographs the C.I.B. on occasion has removed items, such as suspected drugs, for subsequent confirmation. On the Security Service side, the cases of Operation Bricole and Operation Ham provide specific examples of permanent and temporary removal of objects and documents. In some cases, for example to install a listening device in an automobile, the personal property of a suspect — namely his car — may be removed temporarily and returned without detection.

The purpose of the practice

(a) *Security Service*

6. In July 1978, in public testimony, Assistant Commissioner Chisholm testified as follows:

> Surreptitious Entry is an investigative practice which the R.C.M.P. Security Service has and does utilize in investigations relating to subversion, terrorism and activities of foreign intelligence agents in Canada. This practice has been utilized on a selective basis in excess of 20 years.
>
> (Vol. 69, p. 11093.)

7. Then, by way of identifying the objectives of such entries, he quoted from the Report of the Australian Royal Commission on Intelligence and Security,[1] where Mr. Justice Hope spoke of search procedures as follows:

> 163. There are some special circumstances, other than those described in sections 10 and 8 of the Crimes Act, particularly associated with espionage, when it would be proper for A.S.I.O., if it had the power, to search premises for documents and records. The purpose of such a search would not be to obtain evidence, but to obtain intelligence. Thus if a person has been seen on numbers of occasions associating with a known member of an unfriendly foreign intelligence service it may be quite proper for A.S.I.O. to search premises occupied by that person to see whether there is any document or record which would throw light on the nature of that relationship. If some document or record is found it may establish that the offence of espionage has already been committed, and may show what it is the foreign intelligence officer is seeking. Without going this far it may show that, although the offence of espionage has not yet been committed, the foreign intelligence agent has established, or is in the course of establishing, a relationship with the other person which is likely to result in espionage.

8. Part of Assistant Commissioner Chisholm's testimony as to the need for search powers will now be quoted at length as it describes the purpose of the practice:

> *ESPIONAGE*: . . . Some foreign diplomatic missions provide official cover and immunities for a number of staff personnel who are actually intelligence officers specifically assigned to engage in activities beyond the scope of their official status as recognized by international convention or accord. In addition, some of these foreign countries maintain a second and separate intelligence network involving "deep cover operatives" who also perform intelligence functions detrimental to the security of Canada. In espionage parlance, the latter network is referred to as "Illegal" while the former is designated "Legal"; primarily because the network's personnel are legally in the country under official accreditation rather than under false identity. In both cases these hostile intelligence operatives are highly trained, supported by impressive resources to pursue strategic objectives often spanning decades. Both networks operate mainly to recruit and control people with access to the desired intelligence. Some are also known to possess the technical expertise and equipment necessary to systematically monitor Canadian military and other sensitive communications. Intricate clandestine methodology and the use of sophisticated espionage paraphernalia permits [sic] them to operate in relative security, yet their communications remain vulnerable to some degree inasmuch as the paraphernalia they commonly employ, if discovered, is highly incriminating.
>
> Most intelligence operations are strategic in nature and the positive identification of hostile intelligence officers by the Security Service frequently represents only the beginning of our efforts. It is then necessary to identify other agents acting on their behalf, targets to which they are assigned and the potential damage that may be done to Canada. Accordingly, Surreptitious Entries, selectively conducted, have been and must continue to be a

[1] Australia, *Fourth Report of the Royal Commission on Security and Intelligence* (The Hope Report), Canberra, 1978, paragraph 163.

valuable counter-espionage measure enabling the Security Service to quietly identify and exploit hostile intelligence vulnerabilities.

It is clearly the responsibility of the Security Service in its conduct of counter-espionage operations to discern which foreign missions engage in inappropriate intelligence activities in this country, and to inform the Canadian government so that deterring and countering procedures can be considered at the appropriate time. The mission as a whole does everything to conceal the existence of intelligence operatives, frustrating attempts to distinguish them from among other personnel in their diplomatic mission. While Canadian missions abroad are often required to employ local staff, many of whom are believed to be informants of the state security forces, some foreign missions in Canada generally refuse to hire Canadians and consequently eliminate a potentially valuable source of information to the Canadian Security Service.

In spite of such difficulties, ongoing analysis of the behaviour of mission personnel in Canada, together with other information, contributes significantly to the identification of intelligence officers. This information is used to establish operational priorities and to evaluate potential damage to Canadian security interests. While much information on suspected and known intelligence officers can be generated through other investigative techniques, Surreptitious Entries may provide tangible confirmation of intelligence involvement. Items such as sophisticated electronic devices, antennae, note books, and address books, etc., come readily to mind. As well, they can yield data on the target's status, life style, personality, intelligence interests and cover story inconsistencies, all of which contributes to the accurate evaluation of the intelligence officer.

The entry must be surreptitious by its very nature for, if our activities become known to the intelligence officer, he would in all likelihood alter his intelligence activities and possibly hand over the operation to a colleague unknown to us. Of equal importance, knowledge of the entry would provide the opposition with valuable intelligence as to our current counter-espionage capabilities and frustrate our attempts to gain intelligence about their activities and safeguard Canadian interests.

The investigational complexities of detecting illegal networks are even greater, primarily a result of the sophisticated clandestine procedures employed. Any indication that his activities are under investigation will immediately cause an illegal agent to cease operations and, if the danger of exposure is high, flee Canada after destroying incriminating evidence. As with the legal network, the identification of the illegal agent is merely the first step in an operation designed to identify the complete illegal network targets and evaluate the potential damage to Canadian security interests.

To function, the illegal agent must employ communications equipment and other paraphernalia such as code books, one time pads, micro dot readers, secret writing materials which are elaborately concealed when not in use. Clearly, a Surreptitious Entry of a suspected illegal agent's premises may, in some instances, be the only productive technique for confirming or disproving his role. Therefore, it can be a vital tool to effectively prove the existence of an illegal agent operation.

As an investigative tool in counter-espionage operations, Surreptitious Entries are used prudently. Given the practice of intelligence officers being

conscious of potential entry of their premises, there is considerable risk which must be balanced against the potential gains. Nevertheless, after most careful consideration, Surreptitious Entries may in some instances be the only course of action which will provide a material contribution to an important espionage investigation.

SUBVERSION: Subversive activity is normally conducted in a covert manner and usually involves an underground apparatus or rigidly disciplined cells. The immediate problem of gathering intelligence in this situation is evident and can be further complicated when a foreign power fosters and exploits a subversive group as a sphere of influence within Canada. All major Canadian centres have at various times had groups who have advocated violence as the means to bring about governmental change in Canada. In most instances, the life of various organizations is relatively short-lived due largely to the lack of popular support. However, their leaders often seek to support, manipulate or exploit other groups which satisfy their own particular political philosophy and subversive objectives.

How is the Security Service, therefore, to penetrate this area of activity? Surreptitious Entry is one such technique available to the Security Service to gather intelligence to ascertain the plans of a subversive group and the extent of foreign interference. It is entirely possible in a particular case that a Surreptitious Entry may be the only reliable means to determine, without the knowledge of the target, the depth of his or her activities in a subversive organization.

TERRORISM: ... Surreptitious Entry is considered to be a procedure entirely consistent with a "Domestic Security Surveillance Program" leading towards the identification of those committed to terrorism and other acts of political violence.

(Vol. 69, pp. 11095-11103.)

9. Mr. Justice Hope recognized that "although collected as intelligence, some material obtained in such a search may later be used as evidence" in a trial. This is theoretically so in Canada as well, but the likelihood of its occurring is slight, as in the normal case, prosecution is the last thing in the minds of the Security Service investigators; they are likely to be more interested in avoiding prosecution and thus enabling their continued surveillance of contacts made by the targetted person.

10. Assistant Commissioner Chisholm stated that

> As an investigative practice, Surreptitious Entries are only undertaken when other avenues of investigation have failed or are unlikely to succeed in the production of the intelligence required.
>
> (Vol. 69, p. 11094.)

Thus, for example, the contents of documents may be ascertained without surreptitious entry if the Security Service has a paid or voluntary source who has a lawful right to be on the premises. The source may have achieved a position in the organization under scrutiny, and so have access to documents of the kind that the Security Service is interested in.

(b) *C.I.B.*

11. The C.I.B. considers surreptitious entry techniques to be an essential part of the process of electronic interception. It is not necessary here to reiterate in

any detail the reasons for using telephone taps and listening devices in criminal investigations. The points advanced before us to support the need for this technique were made by the C.I.B. and others during the almost ten years of public and Parliamentary discussion which preceded the enactment of the Protection of Privacy Act, which introduced Part IV-1 of the Criminal Code effective July 1, 1974. The C.I.B. concluded that the provision in that legislation for judicial authorization to intercept communications during the investigation of many offences implied parliamentary acceptance of the need for surreptitious entry to install listening devices, and monitoring, repairing and removing them. It was also considered by the C.I.B. (at least until the decision of the Manitoba Court of Appeal in *R.* v. *Dass*[2]) that a court order authorizing the interception of oral communications within premises, even if it contained no express term authorizing entry, *implicitly* gave the right to enter the premises to install devices to implement the interception. The grounds for this conclusion are examined more closely in section D of this chapter.

12. In the case of some kinds of offence, notably in the drug, alcohol and commercial crime area, some of the key persons involved are generally described as sophisticated 'white-collar' types or 'organized crime' types. Either the nature of the crime or the cunning of the persons involved will sometimes make it unlikely that electronic surveillance will provide the desired information or evidence. Therefore it is not surprising that the justification of the use of surreptitious entry for electronic surveillance before 1974 was also invoked both before and after 1974 (indeed until our work was fairly well advanced) to justify surreptitious entry unconnected with electronic surveillance. Surreptitious entry was considered to be justified when the purpose of the entry was to secure information or to confirm that an offence was in the planning stage, or was being or about to be committed, even though a search warrant could not be obtained because there were not reasonable and probable grounds of belief, as required by section 443 of the Criminal Code. In addition, on some occasions where a search warrant might well have been obtained, surreptitious entry without warrant was used because the police needed to ensure, before formal entry and seizure under a search warrant, that the activity under surveillance had reached a stage that the evidence found upon the search would be in such a form as to support a successful prosecution. This type of entry has been described by a C.I.B. witness as a method of conducting an "intelligence probe" (Vol. 36, pp. 5779-80). While such surreptitious entries for criminal investigation purposes have now been prohibited within the C.I.B. pending the Report of this Commission, the R.C.M.P. has submitted that they should be authorized by law in circumstances similar to those in which interception of private communications is authorized.

13. There is also the situation in which there is not only an intelligence probe but the removal of some article from the premises. Examples that are in the public domain were given in the report made by the Deputy Attorney General of British Columbia in December 1978, to which reference will be made in section C of this chapter. That report described four cases in which members of

[2] [1979] 4 W.W.R. 97.

the R.C.M.P. had entered premises without the knowledge of the occupant or lawful authority and had taken an object away with them. They are:

(a) In an investigation of theft from the mails being transported by an airline, a locker which was the property of an airline employee was opened and a pair of pliers was removed. It was suspected that the pliers had been used to create false crimp impressions for postal seals.

(b) While in a place where a listening device was being installed pursuant to an authorization granted by a judge under section 178 of the Code, the members made a search and found a letter in the Chinese language, which they removed and retained. The letter was "to be used in evidence" and therefore presumably had evidential value. However, the accused pleaded guilty. Consequently, no evidence had to be introduced.

(c) In a counterfeit investigation, an interception of a communication pursuant to an authorization under section 178 revealed that counterfeit money was located in a warehouse. As a result an entry was made into the warehouse. Two boxes were found, containing counterfeit United States $20 banknotes with a face value of approximately $1,300,000. They were taken away, some samples were retained, and the balance of the banknotes were returned with secret ultra violet pencil marks placed on some of the notes and on the boxes. The R.C.M.P. commented to the Department of the Attorney General that, while a search warrant might have been obtained, the investigator may have been reluctant to obtain a search warrant because the investigation was still continuing and it was essential to prove knowledge and control of the money on the part of the counterfeiter.

(d) A person was suspected of making obscene movies using juvenile and adult females. It was suspected that he used an apartment for the purpose. The premises were entered in order to substantiate that the suspect was, in fact, engaged in the activity. Several negatives were removed and prints made by the Identification Branch, and the negatives were then returned to the premises in question the same night. Once prints were made of the negatives, steps were then taken to identify the unknown females, especially the juveniles, so that evidence relating to the making or distribution of obscene material under section 159 of the Criminal Code could be gathered. While the foregoing steps were being taken the subject left the area. Upon his return, approximately ten months later, the investigation was re-activated, a search warrant was obtained and search was effected at premises where the obscene material was suspected to be located. The material had been moved from the office darkroom. The suspect was charged with three counts under the Juvenile Delinquents Act. He was convicted, sentenced to five months imprisonment, placed on probation for 18 months with psychiatric treatment ordered.

B. R.C.M.P. POLICIES CONCERNING SURREPTITIOUS ENTRIES — SECURITY SERVICE AND C.I.B.

(a) *Security Service*

14. The Security Service has had detailed operational policies in writing for the use of investigative techniques involving surreptitious entry since the

beginning of the use of technical aids. The following description is based on the testimony of Assistant Commissioner Chisholm (Vol. 69, pp. 11103 et seq.).

15. Until 1959 these techniques could be authorized by the officers in charge of the Security and Intelligence units at the divisions without the need for prior approval from Headquarters. In that year entries for intelligence probes (i.e. to obtain intelligence about documents or objects) were suspended pending a re-examination of the use of such techniques. In 1959, the suspension was lifted and a policy was established which required that the Director of Security and Intelligence (D.S.I.) should approve a surreptitious entry before it took place. An exception was permitted for short-term microphone installations when urgency precluded prior authorization. These operations could be authorized by the officer in charge of a unit in the field.

16. This policy applied until 1966. At that time a moratorium was placed on intelligence probes as such but not upon wiretaps or microphone installations. The moratorium continued for three years until 1969, but even during this period the policy indicated that individual proposals from the field would be considered by the D.S.I. on their individual merit. It is interesting to note that the moratorium coincided with the period during which the Royal Commission on Security was studying the Security Service. That Commission did not refer in its Report to surreptitious entries for the purpose of intelligence probes.

17. In 1969, the D.S.I. lifted the moratorium on surreptitious entries and permitted proposals to "intercept documentary and physical intelligence" to be considered on their individual merit.

18. Since 1971, a Headquarters policy direction has provided that all surreptitious entry techniques require the approval of Headquarters, except that the policy allows for individual discretion in urgent situations to be exercised by officers in charge of Security Service units in the field; reports of all such activities were to be forwarded to Headquarters as soon as possible after the fact. Until June 1974, this policy also applied to surreptitious entry for the installation of listening devices.

19. Since July 1, 1974, the policy with respect to surreptitious entry procedures for the purpose of interception of communications has required compliance with section 16 of the Official Secrets Act. This is a subject that will be considered separately under "Electronic Surveillance" in Chapter 3 of this Part. It need not be discussed in detail here, for no special policies or procedures have been developed that differentiate between the interception of telephonic communications and the interception of other communications. In particular, no express provision for entry into premises has been included in the warrants issued by the Solicitor General under section 16 of the Official Secrets Act.

(b) *C.I.B.*

20. On the C.I.B. side, the development of policy on surreptitious entries apparently was restricted to the use of such entries for installing a listening

device on a telephone or installing a microphone elsewhere on the premises. There does not appear to have been any development of policy concerning intelligence probes.

21. Although the use of 'technical aids' — that is, listening devices — began as early as 1936, the first comprehensive policy covering their use was issued to all operational divisions in 1963 (Vol. 33, pp. 5393-5). This required that technical aids might be used to gain intelligence "to support continued investigations for prosecution" if the intelligence was not available through "usual sources". The policy also recognized that in "abnormal circumstances" technical aids could be used to obtain evidence vital to prosecution. (The reluctance to use such aids was due to a desire to avoid public disclosure of the technique so far as possible.) The policy distinguished between minor and major installations. Minor installations were "routine-type overnight or several-day microphone installations" which could be authorized by the Division Commanding Officer or his designate. Major installations were those involving extensive and complicated technical installations. All major installations had to be submitted to Headquarters for authorization. In early 1964 this policy was supplemented by a requirement that all minor installations were required to be reported to Headquarters.

22. A fully revised policy was issued in 1967, dealing much more extensively with security requirements and limitations upon the use of information received. These additions were felt to be necessary because of increased publicity given to the use of technical aids. The policy did not emphasize pre-requisite conditions to the use of technical aids: it did add to the policy on minor installations a provision that, while such installations could be made in commercial premises, hotels and motels, they could only be extended to private residences with the consent of the occupants. All other residential installations were to be defined as major installations, regardless of the intended duration.

23. In January 1973 a further revised policy on surreptitious entries was implemented, containing criteria as set out in the Protection of Privacy Act then before Parliament, namely that other investigative procedures had been tried and failed, or that they were unlikely to succeed, or that the urgency of the matter was such that it would be impractical to carry out the investigation using only other investigative procedures. The distinction between minor and major installations with respect to private residences was removed. Minor installations were limited to 30 days and a new qualification with respect to the difference between minor and major installations, based upon degree of security risk, was introduced.

24. Since July 1, 1974, the provisions in Part IV.1 — that is, section 178 of the Criminal Code — with respect to judicial authorization have dictated the policy of the C.I.B. governing the use of technical installations.

25. The evidence indicates that no formal or written policy with respect to intelligence probes existed in the C.I.B. before the work of this Commission of Inquiry began.

C. EXTENT AND PREVALENCE OF THE PRACTICE OF SURREPTITIOUS ENTRY

(a) *Security Service*

26. The evidence before us shows that, according to the R.C.M.P., there were 47 entries made from 1971 to February 1978, "to intercept documentary or physical evidence" (Vol. 69, p. 11094). The word 'intercept' is intended to cover cases in which entry was made to search for documents and objects and to inspect and photograph them. We have examined these 47 cases, which include such well-known examples as Operation Bricole (the A.P.L.Q. case) and Operation Ham (the P.Q. tapes case), although in most of the cases our examination of the files has been aimed at determining the objectives and the general circumstances of the operations. In the 47 cases, there were in fact only 34 targets, but in the case of 13 of those targets two surreptitious entries were made. Two of the entries included in the 47 were really not intelligence probes: they were for the purpose of surveying the premises preparatory to installing a listening device. In the field of counter-espionage and the detection of foreign interference, premises and baggage were searched in 17 cases; in six of those the paraphernalia of a foreign intelligence agent, or documents relevant to espionage activity, were found and examined. In counter-terrorist work, ten cases involved searches of premises and baggage, one of which was a case of "rummaging" while a listening device was being installed. One case involved a search of a domestic organization believed to be subversive and suspected of being financed by foreign sources. One case (Operation Ham) involved search of premises in order to gain access to a computer tape belonging to a domestic political party, the tape being temporarily removed in order that it could be copied. One case involved a search of baggage in circumstances in which the activity of the target was possibly outside the mandate of the Security Service. In addition to the 47 cases summarized, we have examined the file relating to one other search; that of a person's residence more than ten years ago. The purpose of that search was to determine whether money from foreign sources was kept on the premises searched.

27. In 1977 and 1978 there were only two completed PUMA operations — one each year (PUMA was the Security Service codeword for surreptitious entries to inspect what could be found on premises). In the previous six years the number carried out averaged seven a year (Vol. C88, p. 12119). Mr. Dare testified that the reason there were so few PUMAS in 1977 and 1978 was that there was no operational need for them during that time (Vol. C88, p. 12122). However, after an adjournment in the hearing he asserted that there is an operational need for PUMAS (Vol. C88, p. 12145). He also said that after the publicity generated by the charges which gave rise to and were made during the course of this Commission of Inquiry, "we became terribly, terribly careful". He added "we have been literally squeezing the operational system" and "we have been constraining ourselves".

28. The cases of which summaries were provided to us included a case which occurred during the past decade, which was referred to in guarded terms in Chief Superintendent Cobb's early testimony (Vol. 10, p. 1353). It was a case

outside Quebec, in which Chief Superintendent Cobb was in no way involved. We have examined the circumstances. They involved entries into the same premises on two occasions, in an attempt to locate and examine certain paraphernalia of espionage. The entries occurred during the early months of the operation of section 16 of the Official Secrets Act. The Solicitor General had granted warrants under section 16 for the interception of telephone conversations and the installation of a "bug". It was purportedly in reliance on these warrants that the entries were made. Documents were photographed and an article was taken away and kept. The Solicitor General was not advised of the entries, nor of the intention to search. The members of the Security Service who planned and authorized the search did not intend in advance that anything be removed from the premises.

29. In addition to entries for the purpose of examining documents and objects, entries have been made to install listening devices (microphones). These include entries to determine the feasibility and mechanics of a possible installation, entries to make an installation, entries to check a device, to effect repairs, and to remove a device. Before July 1, 1974, there were many such installations and, consequently, many such entries. Statistics placed by the R.C.M.P. before the Standing Committee on Justice and Legal Affairs in June 1973, when that Committee was considering the Protection of Privacy Bill, showed that in 1972 the Security Service had made 42 major microphone installations (17 were said to be in counter-espionage, 25 in counter-subversion) and 42 minor installations (23 in counter-espionage, 19 in counter-subversion). The statistics did not indicate whether these entries involved trespass.

30. As for the installation of microphones during the period from 1971 to February 1978, Assistant Commissioner Chisholm testified that there were 223 long-term listening devices and 357 short-term devices (Vol. 69, p. 11094). However, as has been stated earlier, entry is not always necessary for electronic eavesdropping to take place. For that reason, and because there has been no specific requirement to report entries made during the installation of a listening device, the exact number of entries made during that period could not be determined. However, he testified that a review of the files in which the 223 long-term devices were installed indicated that there had been 55 instances of entry. There is no breakdown of those cases into those preceding and those following the implementation of the Protection of Privacy Act. Nor is there any indication as to whether some of those entries were not trespassing, in the sense that consent of an owner, or of an occupant entitled to give consent, had been obtained.

31. Since July 1, 1974, the policy of the Security Service has been that no microphone installations are to be made unless a warrant for interception of "oral communications" has been granted by the Solicitor General under section 16 of the Official Secrets Act. In the year 1978 (for example) 128 warrants for the interception of oral communications were issued. (This figure includes all those in effect during 1979, that were renewed in December 1978.) Many of these interceptions required trespassory entry to be made: none of the warrants expressly authorized entry. Consequently, the authority for lawful entry, if it existed, must have rested upon the operation of section 26 of the

Interpretation Act or section 25 of the Criminal Code. This issue is discussed at length in Chapter 3 of this part of our Report.

32. Finally, since July 1, 1974, there has been a tendency on the part of the Security Service to regard section 16 of the Official Secrets Act as affording a means of obtaining lawful authority for surreptitious entry for the purpose of search, examination and photography on the premises. Clearly it would be improper to apply to the Solicitor General for a warrant under section 16 where the real object of those who seek the warrant is not to intercept communications but to make a search of the premises.

(b) *C.I.B.*

33. From 1963 onward, the installation of listening devices required the approval of Headquarters. From that time records were kept at Headquarters relating to 82 major installations. Not all of these required entries: some required more than one. The records from 1963 to June 30, 1974, (when the Protection of Privacy Act came into effect) showed that there were the following major installations:

	Installations	Entries
"A" Division (Ottawa)	4	7
"C" Division (Quebec)	43	60
"D" Division (Manitoba)	3	5
"E" Division (British Columbia)	10	10
"F" Division (Saskatchewan)	1	5
"H" Division (Nova Scotia)	3	4
"K" Division (Alberta)	6	11
"O" Division (S.W. Ontario)	13	21
	83	123

During the same period there was a record of 3,336 minor installations involving 995 entries:

	Installations	*Entries*
"A" Division	179	15
"B" Division (Newfoundland)	104	7
"C" Division	396	61
"D" Division	194	63
"E" Division	469	132
"F" Division	364	93
"G" Division (Northwest Territories)	3	0
"H" Division	207	20
"J" Division (New Brunswick)	101	12
"K" Division	490	169
"L" Division (Prince Edward Island)	43	3
"O" Division	786	420
	3,336	995

The form for reporting minor installations did not distinguish between those made with and those made without the consent of the occupant or owner. Many installations were made in hotel and motel rooms before the suspect occupied the room and with the consent of the hotel manager, so that there was no trespass. Others were made in commercial premises, cells, police cars and interview rooms with the consent of the owner or occupant, so that again there was no trespass.

34. The Annual Reports of the Solicitor General of Canada made under section 178.22 of the Criminal Code have given statistics as to authorizations granted by judges upon applications made by an agent of the Solicitor General of Canada (but not those made by an agent of a provincial attorney general — who makes a separate annual report). These statistics represent the activity of the R.C.M.P. in criminal investigations. These Annual Reports show that the following interceptions by microphone installations were authorized:

1974 (half-year)	51
1975	176
1976	238
1977	226
1978	227
1979	142

35. It was more difficult to ascertain the extent and prevalence of intelligence probes, that is, entries made for the purpose of a search but without the authority of a search warrant or writ of assistance. In early 1978, Headquarters asked each division to provide such information so that the C.I.B. could prepare to present evidence to us. Because case records were non-existent or difficult to locate, Headquarters suggested that the divisions examine the work orders of divisional Security Engineering Sections. The message from R.C.M.P. Headquarters requested information as to the extent of "illegal" surreptitious entry. This request was imprecise because it failed to define "illegal". The result was confusion in the reports from the divisions as to the extent and prevalence of surreptitious entries for the purpose of intelligence probes. (Ex. E-1, Tab 4B.)

36. One Division ("E" Division — British Columbia) replied candidly that it thought the practice was lawful, although there had been some entries which it thought were "perhaps questionable". It then listed hundreds of 'questionable entries', which are referred to below. As far as "E" Division was concerned, intelligence probes were on a legal plane with entering to place listening devices: in each case the entry would not be accompanied by damage or the intent to commit any offence or the commission of any offence, and consequently (it was contended) would not be illegal. (Ex. E-1, Tab 4C.)

37. Apart from British Columbia, negative replies were received from all divisions — not surprisingly, in view of the lack of definition of "illegal" in the request. Consequently a further message was sent by Headquarters, specifically asking for information about any intelligence probes that had been carried out. This resulted in four more divisions responding with information about a

small number of intelligence probes. On April 18, 1978, Assistant Commissioner T.S. Venner testified as to the result (Vol. 36, p. 5811):

"D" Division (Manitoba)	6
"E" Division (British Columbia)	402
"F" Division (Saskatchewan)	1
"K" Division (Alberta)	9

Other divisions replied that there had been none.

38. "F" Division in Saskatchewan described an entry into an office in a hangar at an airport to examine records. "H" Division in Nova Scotia described an instance in August 1974 when, pursuant to an authorization under section 178 of the Criminal Code, an entry had been made to install a listening device and the opportunity was taken to photograph records and correspondence in an open briefcase on the premises. (As the entry itself was assumed to be authorized in law, Nova Scotia is not included in the list of provinces that reported such entries.) "K" Division in Alberta reported that it had identified two intelligence probes into private residences to search for evidence or intelligence to aid Criminal Code investigations, one into a parked trailer to ascertain whether it contained stolen property, six into business premises to determine whether stolen property was stored there, and one into business premises to photograph company records and documents. "K" Division noted that in all cases there was no damage, no theft and no criminal intent.

39. Clearly at least two results required further investigation: British Columbia, which reported so many, and Southwestern Ontario (including Toronto), which reported none. As for British Columbia, that province's Department of the Attorney General conducted an investigation which showed that the huge figure that had been provided to us was not an accurate response to our search for information but the result of a different interpretation. The report by the province's Deputy Attorney General, dated December 11, 1978, shows that the 402 cases were based on work orders of the Security Engineering Section of that Division, but, of these, 212 cases did *not* involve an entry at all and 149 were made pursuant to consent, warrant or authorizing order. That left 41 to be examined, where there had been entry not authorized or provided for by law:

1.	Cases prior to Privacy Act	5
2.	Cases where no evidence of articles or documents removed	32
3.	Cases where evidence of articles or documents removed	4
		41

Of these 41 cases, 12 were in drug investigations, 27 were in criminal investigations and the nature of two was not known. Twelve involved entry into homes or residences, 29 into other types of premises.

40. The Commission's check of the negative reply of "O" Division, (Southwestern Ontario, including Toronto), indicated that, while the reply was based upon a canvass of all divisional units, it was apparent that no detailed records of the Security Engineering Section were available as a starting point. Assistant Commissioner Venner, in correspondence with the Commission, stated as follows:

> In the early 1970s in "O" Division, unlike some other divisions, the use of wiretaps was permitted and controlled at the line officer level, as I have already testified. This investigative aid gave that division an added advantage in combatting organized crime particularly in the drug enforcement field to the extent that in reality it was not necessary to resort to the 'intelligence probe' type of activity.
>
> By reporting no 'intelligence probes', the division is not denying categorically that any were ever undertaken. The fact that we are dependent on human memory, coupled with the knowledge that no ex-members were included in the survey would make such a denial inappropriate. I am satisfied though, that "O" Division conscientiously went about this search for information and took advantage of every method they could devise to pull together a complete picture.
>
> I would only add that, as you know, I was stationed in "O" Division in three capacities during the years 1973 to 1976, i.e. Division Intelligence Officer, Officer Commanding Metro Toronto Subdivision, Officer i/c Drug Enforcement, all operational roles involving close contact with the Sections and personnel who would have been most active in these endeavours. I assure you I can recall no incident which would render the "O" Division response inaccurate.

41. All divisions were faced with the fact that no records had been kept of such entries; any information provided has been volunteered from the memory of members. In the case of divisions such as Ontario and Quebec, are we to infer that, within the memories of members stationed there in early 1978, there had been no instances of the use of search of premises except upon consent or during an arrest or by virtue of a search warrant or a writ of assistance (under the Narcotics and Excise Acts)? We find it hard to imagine that there were no such instances in recent years, in Ontario and Quebec, of the type which were, for example, disclosed by the divisions in British Columbia and Alberta. However, while we may entertain such doubt, we can only speculate as to whether the technique was frequently used in all the divisions across Canada. Nevertheless, the probability that intelligence probes were more excessive before our inquiry began than the figures disclosed to us would indicate, is demonstrated by the following passage in a brief submitted to us by the R.C.M.P.:

> Two R.C.M.P. criminal investigative sections, Commercial Crime and National Crime Intelligence, have resorted to intelligence probes. Their targets were usually people involved in the stock exchange and organized crime fields. Members employed on these duties, particularly supervisory personnel, did not think that intelligence probes were unlawful. This is evident in the knowledge that no document can be found to show that the Force, up to July 1977, ever asked the Department of Justice to provide a legal opinion on this issue.
>
> (Ex. E-1, Tab 4.)

42. That the technique was probably tolerated at all levels of the R.C.M.P., or at least that a blind eye was turned to it, is suggested by the language chosen by the R.C.M.P. in its statement (Ex. E-1, Tab 4) read as testimony by Assistant Commissioner Venner in April 1978:

> The intelligence investigator and his supervisors have been aware that their responsibility to pursue a course of action in the public interest was paramount... This must and has included uncovering intelligence to determine if serious criminal offences were/are being committed or were/are about to be committed. The investigator faced a dilemma. Should he overlook his responsibility and pursue the matter no further? Or should he, in the "public interest" and without *mens rea*, surreptitiously enter the premises controlled by the suspected criminal to determine for certain if he is involved in crime?

He then observed that:

> No court, to our knowledge, has ever examined the legality of a surreptitious entry by a policeman merely to determine if a person was engaged in crime. No clear legislation exists to prohibit or authorize this action.
>
> (Vol. 36, pp. 5774, 5786-89.)

This understanding of the law, from such an experienced officer, is undoubtedly representative of the opinion commonly held in the Force. His view of the state of the criminal law may well be correct, as far as the practical result of a prosecution of the policeman for breaking and entry is concerned. However, his appreciation of the law was, as he himself recognized, limited to the effect of the criminal law. The R.C.M.P.'s prepared statement, by its silence on the effect of the law of trespass, must be considered as treating it as of no account. It is also noteworthy that the prepared statement considered that, without clear prohibitory legislation or Force policy, and because Force policy approved of the use of surreptitious entry in order to install listening devices, an investigator could feel confident that "within limits" surreptitious entry was lawful and that his actions were in the public interest if he acted "with reasonable grounds in the performance of his duties". Finally, we note that the R.C.M.P.'s prepared statement referred to the "paramount" responsibility "to pursue a course of action in the public interest". To us this signifies clearly that the C.I.B. considered that, even though the law might in some uncertain manner constitute an impediment, it was not to stand in the way of a conscientious investigation in the public interest. All these points add up, in our mind, to substantial evidence of wide use of surreptitious entries with the tacit approval of the management of the Force.

D. LEGAL AND POLICY ISSUES — SECURITY SERVICE AND C.I.B.

General

43. Lord Denning said in a book written when he was a trial judge in 1949:

> Let us consider, then, the power to enter a man's house against his will: for this is a power which has been greatly extended of late. It is a power which

> we must watch with care, because, next to our personal freedom, we value most the freedom of our homes. 'An Englishman's house is his castle' we say: and our feelings about it were well summed up by the great Earl of Chatham when he said "The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail — its roof may shake — the wind may blow through it — the storm may enter — the rain may enter — but the King of England cannot enter — all his force dares not cross the threshold of the ruined tenement". These proud words take their legal origin from Magna Carta, when King John promised that no free man should be disseised of his free tenement except by the law of the land. The freedom of an Englishman's house was there put on an equal footing with his personal freedom. Just as the executive could not deprive a man of his personal freedom except when the law permitted, so also the executive could not enter his house except in accordance with the law.[3]

In a case in 1970 he said:

> The common law does not permit peace officers, or anyone else, to ransack another's house, or to search for papers or articles therein, or to search his person, simply to see if he may have committed some crime or other. If police officers should do so, they would be guilty of a trespass.[4]

44. In his book, *Freedom, the Individual and the Law*, Professor Harry Street writes:[5]

> The law has long imposed serious restrictions on the claims of the police to search private premises. A series of cases in the 1760s followed the issuing by the Government of the day of general warrants to search premises, i.e. warrants in which either the person or the property is not specified. In the great case of *Entick* v. *Carrington*, the Secretary of State issued a general warrant to officers who broke into the house of Entick, who was suspected of editing a seditious publication, "The British Freeholder", and seized his books and papers. The Lord Chief Justice of the day castigated the Government's conduct severely and awarded Entick £300 damages for trespass.

45. The actual decision in *Entick* v. *Carrington* dealt with the validity of general warrants (warrants not specifically identifying the things to be seized) and the need for lawful authority for a warrant if the seizure was not to constitute a trespass. More important than the decision itself were these ringing passages from the judgment of Lord Camden, the Chief Justice:[6]

> By the laws of England, every invasion of private property, be it ever so minute, is a trespass. No man can set his foot upon my ground without my licence, but he is liable to an action, though the damage be nothing; which is proved by every declaration in trespass, where the defendent is called upon to answer for bruising the grass and even treading upon the soil. If he

---

[3] Sir Alfred Denning, *Freedom Under the Law*, London, Stevens and Sons Limited, 1949, p. 103.

[4] *Ghani* v. *Jones* [1970] 1 Q.B. 693 at 706; [1969] 3 All E.R. 720 (English Court of Appeal).

[5] Harry Street, *Freedom, the Individual and the Law*, 3rd edition, Harmondsworth, Middlesex, Penguin Books, 1972, p. 23.

[6] (1765), 19 Howell's State Trials 1001, at p. 1066.

> admits the fact, he is bound to shew by way of justification, that some positive law has empowered or excused him. The justification is submitted to the judges, who are to look into the books; and if such a justification can be maintained by the text of the statute law, or by the principles of common law. If no such excuse can be found or produced, the silence of the books is an authority against the defendant, and the plaintiff must have judgment.
>
> According to this reasoning, it is now incumbent upon the defendants to shew the law, by which this seizure is warranted. If that cannot be done, it is a trespass.
>
> Papers are the owner's goods and chattels: they are his dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection; and though the eye cannot by the laws of England be guilty of a trespass, yet where private papers are removed and carried away, the secret nature of those goods will be an aggravation of the trespass, and demand more considerable damages in that respect. Where is the written law that gives any magistrate such a power? I can safely answer, there is none; and therefore it is too much for us without such authority to pronounce a practice legal, which would be subversive of all the comforts of society.

Ever since, it has been accepted that persons invading property commit a trespass unless they can found their actions upon some rule of positive law. Of those arguments for the defence that were advanced and discarded in *Entick* v. *Carrington* one is of particular interest to us — state necessity. This was held not to afford a justification. Lord Camden, C.J. said:

> With respect to the argument of state necessity, or a distinction that has been aimed at between state offences and others, the common law does not understand that kind of reasoning, nor do our books take note of any such distinctions. . .

46. The only situation in which, until then, the common law had recognized a power to search and seize under search warrant was in the case of stolen goods. This concession had been allowed grudgingly by the judges. However, Parliament obviously considered that, while the root principle established in *Entick* v. *Carrington* was not open to question, the need to search in order to obtain evidence should be provided for in additional particular cases.[7] Consequently, in the century or more that followed in England, a number of statutes were enacted that provided for search upon warrant, usually issued by a magistrate, in respect to a number of offences. In England this catalogue of such powers has never been brought together in a single statutory provision. However, in Canada, since 1886, the Criminal Code has contained just such a comprehensive statutory provision in what is now section 443.[8] It allows a justice to issue a warrant for search and seizure if he is satisfied that

> there is reasonable ground to believe that there is in a building, receptacle or place,
>
> (a) anything upon or in respect of which any offence against this Act has been or is suspected to have been committed,

[7] *Ibid.*, p. 1073.

[8] Section 443 is comprehensive in regard to offences under the Criminal Code. There are additional provisions for search found in other statutes, such as the provisions for writs of assistance found in the Narcotics Control Act.

(b) anything that there is reasonable ground to believe will afford evidence with respect to the commission of an offence against this Act, or

(c) anything that there is reasonable cause to believe is intended to be used for the purpose of committing any offence against the person for which a person may be arrested without warrant.

47. It is important to remember that there is not always a trespass if there is entry upon the premises of a person without his consent and without a warrant or writ of assistance. At common law a constable, and even a private citizen, may forcibly enter a dwelling house to terminate an affray,[9] or to prevent an occupant from doing serious bodily injury to another person in the house. The need to prevent personal injury is the justification for the trespass in such cases.[10] In addition the policeman has a power of forcible entry commensurate with his powers of arrest, by virtue of the common law, which was explained in *Eccles* v. *Bourque* by Mr. Justice Dickson of the Supreme Court of Canada as follows:[11]

> . . . there are occasions when the interest of a private individual in the security of his house must yield to the public interest, when the public at large has an interest in the process to be executed. The criminal is not immune from arrest in his own home nor in the home of one of his friends. So it is that in Semayne's Case a limitation was put on the "castle" concept and the Court resolved that:
>
> In all cases when the King is party, the Sheriff (if the doors be not open) may break the party's house, either to arrest him, or to do other execution of the K.'s process, if otherwise he cannot enter. But before he breaks it, he ought to signify the cause of his coming, and to make request to open doors...
>
> ...Thus it will be seen that the broad basic principle of sanctity of the home is subject to the exception that upon proper demand the officials of the King may break down doors to arrest.

48. The common law has also recognized, to a limited degree, that powers to search under a search warrant may be exceeded by a policeman without his becoming exposed to civil liability for trespass. The most recent English case, *Ghani* v. *Jones*,[12] according to L.H. Leigh,

> . . . suggests that a constable can seize from premises which he has entered lawfully, property of evidential value in connection with the crime which he is investigating. This power enables him to seize material of evidential value against the person whom he is investigating or anyone associated with him in the offence.[13]

---

[9] *R.* v. *Walker* (1854) Dears, C.C. 358. *Timothy* v. *Simpson* (1835) 1 Cr. M.R. 758; *Robson* v. *Hallett* [1967] 2 Q.B. 939, [1967] 2 All E.R. 407; *R.* v. *Marsden* (1925) 88 J.P. Jo. 369, *Handcock* v. *Baker* (1800) 2 Bos. P. 260; *Bailey* v. *Wilson* [1968] Crim. L.R. 617.

[10] L.H. Leigh, *Police Powers in England and Wales*, London, Butterworths, 1975, p. 172.

[11] [1975] 2 S.C.R. 739 at 742-3.

[12] [1970] 1 Q.B. 693; [1969] 3 All E.R. 720.

[13] Leigh, *Police Powers in England and Wales*, London, Butterworths, 1975, p. 184.

Moreover, in *Ghani* v. *Jones* earlier cases[14] were explained as deciding that

> . . . a constable lawfully on premises is entitled to take any goods which he finds in the occupier's possession or in his house and which he reasonably believes to be material evidence in relation to the crime for which the occupier is arrested or in respect of which the constable enters. If, while searching, the constable comes upon other property which shows the occupier to be implicated in some other crime, he may, if he acts reasonably, detain such property for a limited period.[15]

As Leigh says,

> The propositions are apparently very wide. They go well beyond the early limitation that only goods described in a warrant or goods which were apt to provide evidence of goods so described could be taken. Instead, they assert a general right to take goods which the police reasonably suspect may implicate the occupier in the crime charged, whether the search is pursuant to a search warrant or incidental to an arrest. This amounts to a considerable extension of the right to search. These rules coupled with the chance discovery rule, are substantial infringements of the rights of the individual. But the rule as stated by the Court of Appeal may be wider still. For if the occupier has on his premises the property of another, and is arrested and the property found pursuant to a search shows that that other is implicated in the occupier's crime, that other's property may also be seized.[16]

The precise extent to which these recent English cases will be applied in Canada, and what their significance is, remains to be seen.[17] We have referred to them here for two reasons: first, to avoid leaving any impression that upon an entry being made pursuant to search warrant the courts have in all circumstances frowned upon the seizure of goods other than those referred to in the warrant; second, to lay a foundation for a discussion later as to whether, when members of the R.C.M.P. — either investigating a crime or on Security Service duty — enter premises to install a listening device under section 178 of the Criminal Code or section 16 of the Official Secrets Act, they are entitled to search the premises.

49. Throughout this chapter the problem is basically to strike a balance between two conflicting social goals. The dilemma was identified by Lord Denning as being how to permit the power to search as one of "the safeguards of freedom" without permitting abuse of such a power to lead "to the search of any man's house and belongings on the slightest pretext — or on none".[18]

50. However, while we accept that there is a need to strike such a balance, we assert emphatically that it is wrong and unacceptable that any Canadian police force should act on the assumption that its members need be concerned only to

---

[14] *Chic Fashions (West Wales), Ltd.*, v. *Jones* [1968] 2 Q.B. 299; [1968] 1 All E.R. 229 and *Pringle* v. *Bremmer and Stirling* [1969] 3 All E.R. 1700.

[15] Leigh, *Police Powers in England and Wales*, London, Butterworths, 1975, p. 187.

[16] *Ibid.*, p. 188.

[17] The cases are analyzed thoroughly in Leigh, *ibid.*

[18] Sir Alfred Denning, *Freedom Under the Law*, London, Stevens and Sons Limited, 1949, p. 6.

avoid criminal offences: there are other illegalities. The policy of the R.C.M.P. has reflected an attitude that entries without consent or warrant or some other positive legal support are permissible because no criminal offence is thereby committed, as if that disposed of the matter. Leaving aside the few provinces that have Petty Trespass Acts, the police are faced with the "illegality" of the law of trespass for which damages may be awarded (at least in the common law provinces — i.e. all provinces except Quebec). The law of trespass is not to be brushed aside as of no account in deciding Force policy. A trespass is a "wrong". It is *wrongful* to adopt policies that countenance and encourage trespass. If the law of trespass is an obstacle to the effective detection of crime, the law should be changed by the appropriate legislative body. Pending change, the law must be respected.

Possible charges arising out of surreptitious entry

51. We shall now examine eleven different grounds on which it might be argued that a surreptitious entry for one purpose or another constitutes an offence under the Criminal Code or is for some other reason an act "not authorized or provided for by law". All of the following issues except (c), (i) and (j) are issues arising in the criminal law. As will be seen, there are no easy answers as to whether, in conducting a surreptitious entry and search, a policeman commits a crime. We examine those questions in considerable detail, because we consider that it is important that the arguments for and against criminal liability be examined seriously by us. However, we have no hesitation in saying that surreptitious entry will frequently constitute civil trespass, and as we have said, that — at least in the common law provinces — is conduct "not authorized or provided for by law" and therefore not to be permitted, as a matter of policy, unless the law expressly permits it in the circumstances.

(a) *Breaking and entering with intent to commit an indictable offence*

52. The relevant provisions of the Criminal Code are as follows:

306. (1) Every one who

(a) breaks and enters a place with intent to commit an indictable offence therein,

(b) breaks and enters a place and commits an indictable offence therein, or

(c) breaks out of a place after

(i) committing an indictable offence therein, or

(ii) entering the place with intent to commit an indictable offence therein,

is guilty of an indictable offence and is liable

(d) to imprisonment for life, if the offence is committed in relation to a dwelling house, or

(e) to imprisonment for fourteen years, if the offence is committed in relation to a place other than a dwelling house.

(2) For the purposes of proceedings under this section, evidence that an accused

(a) broke and entered a place is, in the absence of any evidence to the contrary, proof that he broke and entered with intent to commit an indictable offence therein; or

(b) broke out of a place is, in the absence of any evidence to the contrary, proof that he broke out after

(i) committing an indictable offence therein, or

(ii) entering with intent to commit an indictable offence therein.

(4) For the purposes of this section, "place" means

(a) a dwelling-house;

(b) a building or structure or any part thereof, other than a dwelling-house;

(c) a railway vehicle, vessel, aircraft, or trailer...

307. (1) Every one who without lawful excuse, the proof of which lies upon him, enters or is in a dwelling-house with intent to commit an indictable offence therein is guilty of an indictable offence and is liable to imprisonment for ten years.

(2) For the purposes of proceedings under this section, evidence that an accused, without lawful excuse, entered or was in a dwelling-house is, in the absence of any evidence to the contrary, proof that he entered or was in the dwelling-house with intent to commit an indictable offence therein.

308. For the purposes of sections 306 and 307,

(a) a person enters as soon as any part of his body or any part of an instrument that he uses is within any thing that is being entered; and

(b) a person shall be deemed to have broken and entered if

(i) he obtained entrance by a threat or artifice or by collusion with a person within, or

(ii) he entered without lawful justification or excuse, the proof of which lies upon him, by a permanent or temporary opening.

53. There can be little doubt that almost all surreptitious entries involve physical "breaking" within the meaning attributed to the sections. Merely opening a closed door and going inside has been held to constitute breaking. Even entrance through an open doorway of a partly constructed unoccupied dwelling-house has been held to constitute constructive breaking under section 308(b)(ii).[19]

54. Section 2 of the Criminal Code defines "dwelling-house" as including any part of a building "kept or occupied as a temporary residence". That would or might include hotel rooms, depending on the circumstances: a long-term hotel guest might be said to have his temporary residence there, but there is more uncertainty about a short-term guest. Assuming the room to be a "temporary residence", is there a "breaking and entry" of a "dwelling-house" if the hotel owner or his employee consents to the entry and provides a key? There appears to be no authority in Canada dealing with the provision of a pass-key by those

[19] See the cases discussed in Mewett and Manning, *Criminal Law*, Toronto, Butterworths, 1978, p. 510.

in charge of hotels or apartment buildings. Courts in the United States have distinguished the status of a tenant who acquires a property interest from that of a hotel guest. The hotel guest in those cases has been considered to be a mere licensee, while the owner remains the occupier as he must look after the hotel room and has access for that purpose. Yet entry by pass-key has been held to be 'breaking' in both situations.[20] Whether or not the courts in Canada will find constructive breaking by pass-key under 308(b)(i) or in general law is speculative. The foregoing discussion applies to an occupied hotel room. What about a hotel room that is not yet occupied by the suspect? When the entry is made, with the consent of the owner or his employee, for example to install a device before the suspect arrives, there would not appear to be any possible application of the section.

55. The most substantial doubt as to the presence of all ingredients of the offence arises from the requirement that there be an "intent to commit an indictable offence" in section 306(1) and the provision "without lawful excuse" in section 307. Sections 306(2)(a) and 307(2) raise a presumption of intent "in the absence of evidence to the contrary" once there is evidence of breaking and entry or that the accused is in a dwelling-house "without lawful excuse". Three preliminary points should be noted with respect to this presumption:

(a) Cases prior to 1969 are of little assistance since the sections then made evidence of break and enter "*prima facie* evidence" of intent, instead of providing that a presumption of intent exists.

(b) The presumption is rebutted if, in all the circumstances of the case, the explanation of the accused could reasonably be true even if the trier of fact is not convinced that it is.

(c) Once the presumption is rebutted by evidence to the contrary, the normal burden of proof beyond a reasonable doubt is imposed upon the prosecution.[21]

Thus if the intent of a surreptitious entry is to obtain information there would appear to be no offence under sections 306 and 307 unless an indictable offence is actually committed following a breaking-in, or preceding a breaking-out. The same conclusion would appear to apply to what occurred prior to July 1, 1974, if the intent was to wilfully intercept a private communication by means of placing a listening device in premises. In one case where a private detective took three assistants for an entry to take photographs, the court found an intention to commit an indictable assault[22] but, in the absence of some such special circumstance, it would appear that the trespass would not result in a conviction under sections 306 or 307.

56. Since the commencement of our work there has been a number of statements in the media that members of the R.C.M.P. who have entered

---

[20] *Smith* v. *Director, Patuxent Institution* (1973) 395 F. Supp. 813 (U.S. D.C. Maryland); *Jack* v. *United States* (1967) 387 F. 2d 471 (U.S. Ct. of App., 9th Circ.); *Buck* v. *Del City Apartments* (1967) 431 P. 2d 360.

[21] *R.* v. *Marshall* (1971) 1 C.C.C. (2d) 505; (B.C.C.A.); *R.* v. *Rivera* [1975] 2 W.W.R. 56 (B.C.C.A.).

[22] *R.* v. *Massue* [1966] 3 C.C.C. 9 (Que. C.A.).

premises without consent or a warrant to conduct an 'intelligence probe' have been guilty of breaking and entry ("B & E"). Such assertions are not necessarily correct. If a member entered premises in order to search for drugs or a counterfeit printing press when he did not have the grounds of belief to enable him to swear the information necessary to obtain a search warrant and he did not have a warrant, or if he entered premises to look for espionage paraphernalia or to look at documents, or if, before July 1, 1974, he entered for the purpose of installing a listening device, he would be convicted only if he failed to testify as to his reason for entering. If he did not testify, so that the only evidence before the court was that he broke and entered, the presumption would normally lead to his conviction. However, if he testified, and if he were believed (as would likely be the case), he would not be convicted, because he did not enter with the intent to commit an indictable offence in the place. In saying this we assume that he did not cause any damage; usually he would not do so as he would wish the suspect to be unaware of the search. The small likelihood that a member of the R.C.M.P. would be convicted of breaking and entry with intent to commit an indictable offence in the place entered is illustrated by what was said by Mr. Justice J.K. Holmes in a recent address to the jury in the Court of Queen's Bench of Alberta. In a trial in 1980, at Calgary, the accused, Claude Wagner, was convicted of break, enter and theft, and, on a separate count, of mischief. Those facts that are relevant for our purpose are set forth in the judge's summing up. The accused, a private citizen, had entered a dwelling-house occupied by two persons by pushing open an unlocked but closed window, and removed some documents. A witness for the prosecution testified that he and the accused planned to deceive a Calgary city police detective. The accused denied this. The detective testified that the entry, in the planning of which he had participated, was for the purpose of Wagner searching for illegal drugs. The detective testified that he was surprised when the accused later produced the documents which he took from inside the house. Mr. Justice Holmes told the jury:

> At this point I would like to comment on a matter which arises from Crown counsel's opening address to you, before any evidence was called. He made a comment to the effect that it was not a criminal offence for the police to make an unauthorized entry of premises only for the purpose of searching a place to assist the police to obtain information. *Such a procedure would certainly not constitute an offence under the Criminal Code of Canada* although it may not find approval by all members of our society. However, it is not your function to determine whether you agree as a jury on this case with the police tactics which were used and which were revealed in the evidence. (our emphasis added)

Therefore in these cases, even if, through more detailed investigation of the individual cases than we have conducted, evidence admissible in court were available to establish the breaking and entry, the attorney general of the province would have to decide whether the likelihood of conviction justified a prosecution in the light of what we have just pointed out. (In a subsequent Report we shall discuss the factors that should be taken into account in deciding whether to prosecute.)

57. There is another point to be made about this offence. The fact that the law makes conviction of a policeman engaged in such duties most unlikely has been misconstrued by some members of the R.C.M.P. They tend to construe the reason for likely acquittal as being that the policeman lacks "criminal intent". In a sense that is true; he lacks the intent *to commit an indictable offence* in the place. But what they really mean is that they think the criminal law would excuse him because he does not "intend" to commit any crime. From this proposition they infer that if he does any other act which, if done by an actual criminal to serve his own ends would be a crime, the policeman is not guilty of the same crime because he does not intend to commit a crime. This is a fallacy. It rests upon a distortion of the doctrine of *mens rea*, to which they have been first introduced in their training in Regina. They confuse *mens rea* (the general intent to do the act, which is an element of criminal liability) with the intent to commit a crime (i.e. to do the act for ignoble ends). The law is that if an accused does an act with noble purposes — whether he is a policeman or an ordinary person — that is no defence, provided that he did intend to do the act.

58. This erroneous reasoning appears to be firmly rooted in the R.C.M.P. and to have broad currency. It generates an attitude of mind that tolerates acts committed for such noble purposes as "the public interest" or "the protection of the security of the state", that if committed for other purposes the policemen themselves would regard as offences. It is therefore a dangerous heresy that must be overcome in the education and training of members of the Force and not allowed to persist in their thinking or in that of the members of a security intelligence agency.

(b) *Wilful disobedience of a statute*

59. As a result of the entry onto the premises of the Agence de Presse Libre du Québec on October 6 and 7, 1972, a member of the R.C.M.P. (Inspector Donald Cobb), a senior member of the Sûreté du Québec and a senior member of the Montreal Urban Police Force entered a guilty plea in May 1976, to a charge which was laid against them under section 115 of the Criminal Code. That section reads as follows:

> 115. (1) Every one who, without lawful excuse, contravenes an Act of the Parliament of Canada by wilfully doing anything that it forbids or by wilfully omitting to do anything that it requires to be done is, unless some penalty or punishment is expressly provided by law, guilty of an indictable offence and is liable to imprisonment for two years.

60. The section requires three elements to constitute an offence:

(a) a contravention of an Act of the Parliament of Canada which forbids some act or requires an act to be done;

(b) no penalty or punishment provided for the contravention of the statute concerned; and

(c) the accused's act or failure to act must have been wilful and without lawful excuse.

61. The offence with which these officers were charged was that they had contravened section 115 of the Code "by wilfully omitting to do something which section 443 required to be done: obtaining a warrant under section 443 of the Criminal Code". It is difficult to understand that charge. Section 443 does not *prohibit* the act of search and seizure without a warrant, or *require* an application to be made for a warrant. It merely provides a comprehensive procedure for applications for, and the issuing of, warrants for search and seizure in the three situations referred to in the section. There is no prohibition of an act or of an omission to do an act. In our opinion the provisions of section 115 do not constitute a basis for criminal liability for search and seizure without warrant. It may seem strange to the reader that we are saying that Inspector Cobb and the others pleaded guilty to an offence which, in the circumstances, did not exist, but that is indeed our opinion.

(c) *Petty Trespass Acts*

62. The legislatures of all provinces except Saskatchewan, Nova Scotia and Prince Edward Island have enacted legislation making a trespass in certain circumstances a summary conviction offence. Being summary conviction offences, prosecutions must be launched within six months (section 721, Criminal Code). The Petty Trespass Acts of British Columbia[23] and New Brunswick[24] apply to such narrow factual situations as to be irrelevant to criminal investigations and security intelligence work. Likewise, Quebec has a statute[25] that may appear to be broadly applicable to all "land" (*terrains*) but its scope is probably restricted to the kind of land referred to in the title of the statute: the Agricultural Abuses Act. The Petty Trespass Acts of Alberta,[26] and Newfoundland[27] apply only where a form of notice not to trespass has been posted; they therefore are irrelevant to the usual intelligence probe of a house or apartment. We are left with Ontario and Manitoba. Until 1980, the Ontario Petty Trespass legislation applied to any "enclosed" land and therefore did not apply to an open parking lot or to "open" parking garages under buildings. However, it applied to houses, apartments and offices, and therefore was of importance to the ability of a police force or to the Security Service to perform its tasks in cities such as Ottawa and Toronto. The new Trespass to Property Act, 1980,[28] likewise prohibits unauthorized entry onto premises "enclosed in a manner that indicates the occupier's intention to keep persons off the premises...". Similarly, the Petty Trespass Act of Manitoba[29] creates an offence when any person "unlawfully enters into. . . any land or premises. . . being the property of another and being wholly enclosed...". A legal problem therefore still faces the R.C.M.P. and other police forces, and any security intelligence agency, when its members enter the kind of premises referred to above.

---

[23] R.S.B.C. 1960 ch.387.
[24] R.S.N.B. 1973 ch.T-2.
[25] R.S.Q. 1964 ch.130 ss. 2,3.
[26] R.S.A. 1970 ch.273 ss. 2,3.
[27] S. Nfld. 1975-76 No. 59, s.2.
[28] S.O. 1980 ch.12. Replaces R.S.O. 1970 ch.347.
[29] R.S.M. 1954 ch.197 s.2.

63. There are many cases dealing with the phrases "enclosed" land, "unlawfully enters" and "acting under a fair and reasonable supposition that he had a right to do the act complained of" which appear in the legislation in some of the provinces.[30] Cases interpreting this latter phrase recognize a mistake of law defence where the belief in the right advanced was a "fair and reasonable" belief.[31] The six-month limitation period of section 721 of the Criminal Code would be applicable, as these are summary conviction offences.

(d) *Theft*

64. In those instances in which surreptitious entry and search by a policeman have been followed by removal of objects or documents from the premises the policeman may be guilty of theft, even if he intends to return what was removed so that the owner or occupant of the premises will not know that anything has happened.

65. The relevant parts of section 283 are as follows:

> 283. (1) Every one commits theft who fraudulently and without colour of right takes, or fraudulently and without colour of right converts to his use or to the use of another person, anything whether animate or inanimate, with intent,
>
> (a) to deprive, temporarily or absolutely, the owner of it or a person who has a special property or interest in it, of the thing or of his property or interest in it,
>
> . . . or . . .
>
> (d) to deal with it in such a manner that it cannot be restored in the condition in which it was at the time it was taken or converted.
>
> (2) A person commits theft when, with intent to steal anything, he moves it or causes it to move or to be moved, or begins to cause it to become movable.
>
> (3) A taking or conversion of anything may be fraudulent notwithstanding that it is effected without secrecy or attempt at concealment.
>
> (4) For the purposes of this Act the question whether anything that is converted is taken for the purpose of conversion, or whether it is, at the time it is converted, in the lawful possession of the person who converts it is not material.

Other policemen who accompany an officer and help him to remove objects or documents, or encourage him to do so may also be guilty. This occurs by virtue of sections 21 and 22 of the Code, which make them parties to the offence.

66. The phrase "fraudulently and without colour of right" in section 283 raises at once the question of the mental state of the accused, which is a necessary element of the offence. "Fraudulently" has been held to mean that the taking must be intentional and deliberate, without mistake and without

---

[30] Alberta s.8, Manitoba s.2, Newfoundland s.6, Ontario s.4 (old Act).

[31] *R.* v. *Davy* (1900) 27 O.A.R. 508; *R.* v. *Malcolm* (1883) 2 O.R. 511; *R.* v. *Burko* [1969] 1 O.R. 598; *R.* v. *Labelle* [1965] 1 O.R. 321 (Ont. C.A.).

knowledge that the property taken is not the accused's.[32] But two decisions in the Ontario Court of Appeal suggest that conduct is not fraudulent merely because it is unauthorized, unless it is dishonest and morally wrong. Thus an honest belief in a moral claim might negate the requirement that a taking be done fraudulently.[33] May a defence of "colour of right" be allowed, even though founded upon an honest belief in the right to act which turns out to be based upon a mistake whether of law or fact? Mr. Justice Rand and Mr. Justice Taschereau held in a Supreme Court of Canada case[34] that in the circumstances of the case (whether logs had been abandoned by a company) since the alleged mistake was a mistake as to the general law, the accused's belief in his "right" (to take the logs) was not admissible as a defence. (They were only two members out of seven. The other members of the court did not discuss the point.)

67. However, a series of cases in the Ontario and British Columbia Courts of Appeal have held that a "colour of right" defence can be supported by an honestly held belief even if founded upon mistake of fact or mistake of law.[35]

68. It might be argued that the phrase "takes... anything whether animate or inanimate" does not include information taken, for example, by photographing documents, and that there is no property right to the information. However, the expanded definition of an "animate and inanimate" thing in section 283(1)(a), which extends the meaning so that it is an offence to deprive a person of his "special property or interest" in the thing, must raise doubt as to the validity of such an argument. Therefore it may be possible to contend that even the photographing of documents on the premises constitutes "taking" a "thing".[36]

69. Some years ago Parliament considered it to be inappropriate that young people should be convicted of an offence as serious as theft when they took a vehicle for a "joyride" but with no intent to keep the vehicle, so that a lesser offence, punishable on summary conviction, was enacted. It is now section 295, which makes it an offence to take a vehicle, without the owner's consent, with the intent to drive it. Does this suggest that in other circumstances, such as taking a document with the intent of copying it and then returning it, there is not a theft but only something less then theft? It cannot be stated categorically that it is theft to remove a document or a thing temporarily from the place where it is kept by the owner, so that it may be examined or copied off the premises and returned before the owner misses it. In a series of Canadian cases,

---

[32] *R.* v. *Brais* (1972) C.C.C. (2d) 301 (B.C.C.A.)—followed in *R.* V. *Renz* (1974) 14 C.C.C. (2d) 492 (B.C.C.A.) and by Mr. Justice Martland in *Lafrance* v. *The Queen* (1973) 13 C.C.C. (2d) 289 (S.C.C.).

[33] *R.* v. *DeMarco* (1973) 13 C.C.C. (2d) 369 (Ont. C.A.); *R.* v. *Hemmerly* (1976) 30 C.C.C. (2d) 141.

[34] *R.* v. *Shymkowich* (1954) 110 C.C.C. 97.

[35] *R.* v. *Howson* (1966) 3 C.C.C. (2d) 348 (Ont. C.A.); *R.* v. *DeMarco* (1973) 13 C.C.C. (2d) 369 (Ont. C.A.); *R.* v. *Scallen* (1974) 15 C.C.C. (2d) 441 (B.C.C.A.).

[36] *Oxford* v. *Moss* [1979] Crim. Law Rev. 119 (Div. Ct.); *R.* v. *Scallen* (1974) 15 C.C.C. (2d) 441 at 473 (B.C.C.A.).

the accused have been acquitted when the evidence did not establish that the accused had the "... intent to deprive the owner of his property either temporarily or permanently".[37] Another line of cases in which theft was held not to have occurred, are the so called 'prank' cases.[38] One Canadian textbook on criminal law states: "If it is intended to take the object temporarily and restore it before the owner misses it or has any use for it, then he has not been deprived of it and theft is not, at that stage, committed".[39] We do not think that the cases support the flat statement contained in that textbook. The most that can be said is that intention is a key factor in the offence and that the courts have held that there are certain types of cases where the necessary intention is not present. In our view none of the types of lack of necessary intention which have been recognized by the courts, to this date, are applicable to the activities of the R.C.M.P. when the latter remove documents or things, copy them and return them, all without the knowledge of the owner.

(e) *Mischief*

70. There may be instances when surreptitious entry is effected by means which involve damage to property, although that seems unlikely since the intention of the investigator would normally be to leave no trace of the entry. However, damage may occur if for some operational reason it is intended to let the suspect know that there has been a search. The problem also arises in the case of the installation of electronic listening devices, which almost inevitably involves some damage to property even if the damage is subsequently concealed. If there is damage to property, the following provisions of the Criminal Code may be applicable:

> 387. (1) Every one commits mischief who wilfully
>
> (a) destroys or damages property,
>
> (b) renders property dangerous, useless, inoperative or ineffective,
>
> (c) obstructs, interrupts or interferes with the lawful use, enjoyment or operation of property, or
>
> (d) obstructs, interrupts or interferes with any person in the lawful use, enjoyment or operation of property.

---

[37] *Cooper* v. *The King* (1949) 93 C.C.C. 286 (N.S. Sup. Ct. en banc). In that case another reason given for acquittal was that the aircraft in question was never moved away from the owner's property.

[38] *R.* v. *Kerr* (1965) 4 C.C.C.37 (Man. C.A.) held that the evidence created at least a reasonable doubt as to whether the accused intended to steal an ashtray. Again, in *R.* v. *Wilkins* (1965) 2 C.C.C. 189 where the accused was held not to have intended to steal the parking meter enforcing officer's vehicle but only to perpetrate a joke and not "to convert the property in it to his own use." The intention only to play a trick and not to steal was also the basis of acquittal where an election poster was taken and placed on the property of the opponent of the candidate whose poster it was: *Handfield* v. *The Queen* (1953) 17 C.R. 343. On the other hand, the view that the fact that it was intended only to carry out a prank is not a ground for acquittal was adopted by the majority of the Quebec Court of Appeal in *Bogner* v. *The Queen* (1976) 33 C.R.N.S. 348.

[39] Mewett and Manning, *Criminal Law*, p. 498.

(7) No person commits mischief within the meaning of this section by reason only that he attends at or near or approaches a dwelling-house or place for the purpose only of obtaining or communicating information.

388. (1) Every one who wilfully destroys or damages property is, where actual danger to life is not involved, guilty of an offence punishable on summary conviction if the alleged amount of destruction or damage does not exceed fifty dollars.

Section 386 provides a definition of "wilfully" for the purposes of Part IX of the Criminal Code as follows:

386. (1) Every one who causes the occurrence of an event by doing an act or by omitting to do an act that it is his duty to do, knowing that the act or omission will probably cause the occurrence of the event and being reckless whether the event occurs or not, shall be deemed, for the purposes of this Part, wilfully to have caused the occurrence of the event.

(2) No person shall be convicted of an offence under sections 387 to 402 where he proves that he acted with legal justification or excuse and with colour of right.

Since surreptitious entries are normally planned to avoid detection it would appear doubtful that subsections (b), (c) or (d) of section 387(1) would become operative. However, physical damage, no matter how nominal, is usually caused by the installation of hidden microphones, and thus sections 387(1)(a) and 388(1) are *prima facie* applicable to those circumstances. Only nominal physical damage is required for the offence to be complete, and the two sections create separate offences.[40]

71. In addition, it can be argued that merely handling chattel property found in the premises amounts to a trespass upon the chattels and is thus an interference with the lawful use or enjoyment of the property contrary to section 387(1)(c). If this is so, then the indictable offence of mischief has been committed. This in turn would mean that if entry had been gained by a "breaking", then an offence under section 306(1)(b) ("breaks and enters a place and commits an indictable offence therein") is also committed, even though it be established that the original break-in was not made "with intent to commit an indictable offence".

72. Subsection (7) of section 387 follows a subsection that exempts stoppage of work situations from "mischief" and therefore subsection (7) might be thought to have been intended to relate to labour-management disputes. The broad language of the subsection might sustain an ingenious defence, for the usual reason for surreptitious entry of a dwelling-house is clearly for the purpose only of obtaining information.

73. If the recent "colour of right" cases, referred to above in our discussion of theft, are followed in defining the ambit of mistake of law or fact as affecting a "colour of right" defence, reliance upon legal opinion (even mistaken ones) or the existence of warrants or authorizing orders under section 178 could also provide the beginnings of a defence. It should be noted, however, that section

[40] *R.* v. *Ninos and Walker* [1964] 1 C.C.C. 326 (N.S.S.C. In Banco).

386(2) requires that an accused prove both legal justification or excuse *and* colour of right. With respect to the requirement of "legal justification or excuse", see below where the cases with respect to "without lawful excuse" are considered in detail. In addition, the criminal law, in certain contexts (e.g. homicide) recognizes a difference between justification and excuse. Whether or not it was intended by the draftsman, either justification or excuse will meet the test of section 386(2). It may well be that the tests applicable to "without lawful justification" will not be the same as those for "without lawful excuse".

74. In respect of entries made since July 1, 1974, to install lawfully authorized listening devices the issue of legal justification or excuse requires consideration of the effect of section 25 of the Code and section 26(2) of the Interpretation Act, which have been relied upon by the R.C.M.P. and its advisers. In Chapter 3 of this Part, while discussing "Electronic Surveillance", we shall examine the effect of those sections and suggest that they are at least doubtful sources of justification or excuse for such entries.

(f) *Trespassing at night*

75. In some circumstances surreptitious presence at night on the grounds of a house, or in the hallways of an apartment building, preparatory to effecting a surreptitious entry into the house or into an apartment, might give rise to an offence under section 173 of the Criminal Code. It provides as follows:

> 173. Every one who, without lawful excuse, the proof of which lies upon him, loiters or prowls at night upon the property of another person near a dwelling-house situated on that property is guilty of an offence punishable on summary conviction.

"Dwelling-house" is defined as follows in section 2:

> "dwelling-house" means the whole or any part of a building or structure that is kept or occupied as a permanent or temporary residence and includes
>
> (a) a building within the curtilage of a dwelling-house that is connected to it by a doorway or by a covered and enclosed passageway, and
>
> (b) a unit that is designed to be mobile and to be used as a permanent or temporary residence and that is being used as such a residence.

"Loitering" means hanging around, and "prowling" means looking for trouble or hunting for an opportunity to carry out an unlawful purpose. There are two offences.[41] If the element of loitering or prowling is present, the defence of lawful excuse cannot be supported on the basis of a right to investigate if carried out by trespass which is itself unlawful.[42] In order to obtain a conviction, the Crown need not prove that the accused had a specific intent. Therefore an accused will be guilty even though he believed he was acting lawfully or even if he was incapable of forming any specific intent.[43] Being a

[41] *R.* v. *Andsten* (1960) 128 C.C.C. 311, 32 W.W.R. 329 (B.C.C.A.); *R.* v. *McLean* (1970) 1 C.C.C. (2d) 277, 75 W.W.R. 157 (Alta. Mag. Ct.); *R.* v. *Edgar & Rea* (1962) 132 C.C.C. 396 (B.C.C.A.).

[42] *R.* v. *Andsten* (1960) 128 C.C.C. 311 (B.C.C.A.).

[43] *R.* v. *Andsten*, *supra*, at 318; *R.* v. *Clark* (1971) 17 C.R.N.S. 56 at 64 (Man. Mag. Ct.).

summary conviction offence, the six-month limitation period, provided for in section 721 of the Criminal Code, would be applicable to "trespassing at night".

(g) *Possession of house-breaking instruments*

76. If a policeman, intending to enter a place of residence or an office surreptitiously and without a search warrant, is in possession of a lock-pick, he may be committing the offence of being in possession of "an instrument suitable for house-breaking". If he is not himself in possession of such an instrument but he brings with him a civilian lock expert who is, the policeman may be a party to the offence. Section 309(1) provides as follows:

> 309. (1) Every one who, without lawful excuse, the proof of which lies upon him, has in his possession any instrument suitable for house-breaking, vault-breaking or safe-breaking, under circumstances that give rise to a reasonable inference that the instrument has been used or is or was intended to be used for house-breaking, vault-breaking or safe-breaking, is guilty of an indictable offence and is liable to imprisonment for fourteen years.

The word "suitable" and the phrase "under circumstances that give rise to a reasonable inference that the instrument has been used or is or was intended to be used for... safe-breaking" were added in 1972.[44] The elements of the offence require proof of suitability, and of circumstances giving rise to one of the reasonable inferences described — namely actual use or present or past intention to use. Once these three elements have been proved, the burden shifts to the accused to establish a "lawful excuse" on a balance of probabilities.[45]

77. Subsection (2) of section 309, which makes it an offence to have a face "masked or coloured or otherwise disguised", expressly provides that, for the offence to exist, the accused must have had the "intent to commit an indictable offence". However, it is not clear whether such an intent is a necessary element for the "reasonable inference" described in subsection (1). It was held in one case that the jury must be asked whether the circumstances gave rise to a reasonable inference that the instrument had been used or was intended to be used for house-breaking, but the court did not define "house-breaking".[46] If house-breaking is the same as "break and enter" as that phrase is used in section 306, there is a further element of intent to commit an indictable offence. The word "house-breaking" has been in the Code for many years without definition, but formerly the context was "instruments for house-breaking". The Code of 1927, however, distinguished between two offences in section 464. Under clause (a), possession, without lawful excuse, of an instrument for house-breaking by night was an offence. Under clause (b), possession of an instrument for house-breaking by day with intent to commit an indictable offence was a separate offence. It is at least arguable that in the 1927 Code house-breaking referred only to break and enter with no element of

[44] S.C. 1972, ch.13, s.25.

[45] *R.* v. *Kozak and Moore* (1975) 30 C.R.N.S. 7 (Ont. C.A.).

[46] *R.* v. *Kozak and Moore*, *supra*, per Martin J.A.

intent, since, in the case of (b), it would be unreasonable to have regarded the word "house-breaking" as meaning the commission of "breaking and entry with intent to commit an indictable offence", for such a definition would have rendered unnecessary the words contained in the express statement of the offence (i.e. "with intent to commit an indictable offence"). If this reasoning is correct, then in the present Code, it is probable that the word "house-breaking" is to have the same meaning — i.e. the fact of breaking and entry without any superimposed intent to commit an offence. Thus possession of such instruments with a mere intent to trespass and no more may be an offence under section 309(1) even when there is no offence of "break and enter" under section 306.

(h) *"Without lawful excuse"*

78. The phrase "without lawful excuse" appears as an element of three offences we have discussed: trespassing at night, being unlawfully in a dwelling-house, and possession of house-breaking instruments. There is no definition for "without lawful excuse" or "lawful excuse" in the Criminal Code despite the importance of the term in construing the scope and application of sections 173, 307 and 309. We now consider some of the cases which may be of assistance in understanding how the phrase, as used in various statutes, has been interpreted by the courts.[47]

79. *Canada*: In *Regina* v. *Andsten*[48] lawful excuse for loitering (section 173 of the Criminal Code) was held to mean an excuse which was lawful under the "law of the land", (i.e. either by common law or statute law). The fact that the private investigators who were the accused in that case were investigating a wife's conduct was held not to be a lawful excuse as it would not be an excuse or justification in a trespass action. In *Regina* v. *Gibson*[49] this same "excuse which is lawful under 'the law of the land' test" was applied in a charge of entering a dwelling-house (section 307 of the Criminal Code). The fact that the accused, a private investigator, had committed the tort of trespass and possibly the tort of invasion of privacy meant that he had no lawful excuse for his entry. In *La Reine* v. *Marché de Québec Inc. and Begin*[50] ignorance of the law prohibiting the importation of American margarine or of the law prohibiting making American margarine appear to have the character of Canadian margarine constituted a lawful excuse for possession of the margarine on a

[47] In addition to the Canadian and English cases that are discussed in the following paragraphs, reference may be made to the considerable jurisprudence in Australia and New Zealand, which includes *Regina* v. *Phillips* (1973) 1 N.S.W.L.R. 275, *Holmes* v. *Hatton* (1978) 18 S.A.S.R. 412, *Killen* v. *Police* [1965] N.Z.L.R. 481, and *Carpenter* v. *Police [1969]* N.Z.L.R. 1052. See also the review of the cases by Anthony Dickey, "Being on Premises 'Without Lawful Excuse' — A Study in Judicial Interpretation", (1973) 47 *Australian L.J.* 382.

[48] (1960) 129 C.C.C. 311 (B.C.C.A.).

[49] [1976] 6 W.W.R. 484 (Sask. District Court). The same view, that private investigators do not, by virtue of their duty to their client to investigate, have a lawful purpose, has been adopted by the Australian cases involving private investigators.

[50] [1969] 1 Ex. C.R. 3 (Exchequer Court).

charge under the *Customs Act*. This case is generally considered to be an anomaly, for ignorance of the law is not usually considered to be an excuse. In the recent case of *Regina* v. *Parrot*[51], the Ontario Court of Appeal held that a "mistaken belief as to one's legal obligation does not constitute a lawful excuse". These cases cannot be said to have resulted in a clear Canadian doctrine as to the extent of "lawful excuse".

80. *England*: In England the Court of Appeal has held that a mistaken belief that the law justifies the accused's act does not constitute "lawful excuse".[52] But there may be a lawful excuse if there is a common law duty to do an act which in normal circumstances would be an offence. An example is carrying a firearm with the intention of surrendering it to the authorities who had invited terrorists to surrender their arms.[53] Another is possession of forged bank notes solely for the purpose of surrendering them to the police — such possession being wholly consistent with the common law duty of a citizen to assist the police in the capture and prosecution of a felon.[54] There may also be a lawful excuse if the accused had an honest and reasonable belief in a state of facts which, if true, would have made his conduct lawful.[55]

81. With the exception of *La Reine* v. *Marché de Québec Inc. and Begin* it appears that Canadian courts and those of other Commonwealth countries have held that ignorance or mistake of law does not constitute a lawful excuse for an accused's actions. Leaving aside mistake of law, whether a member of the R.C.M.P., if charged, as a result of a surreptitious entry, with trespassing at night, being unlawfully in a dwelling-house, or having possession of house-breaking instruments, would be found to be acting "without lawful excuse" would depend on future interpretation of that phrase by the courts. If the strict interpretation of the British Columbia Court of Appeal in *Regina* v. *Andsten* is adopted (that any violation of the law of the land, whether civil or criminal, would prevent the accused from having a lawful excuse) it would be unlikely that a member of the R.C.M.P. could establish lawful excuse on a charge under section 173 (trespassing at night) or section 307 (being unlawfully in a dwelling-house). Applying this interpretation to section 309(1) (possession of house-breaking instruments) would be difficult as the mere act of possessing such instruments would not normally involve a violation of the criminal or civil law, apart from the very provisions of section 309(1). If the narrower interpretation placed on the phrase in a number of Australian cases is adopted, a member of the R.C.M.P. could argue successfully that he had a "lawful excuse" if his conduct gave rise to a mere matter of civil compensation, and he could be convicted only if his conduct were held to be such as to deserve the application of the criminal law — a somewhat subjective question.

---

[51] *Regina* v. *Parrot* (1979) 51 C.C.C. (2d) 539, leave to appeal to the Supreme Court of Canada refused on January 29, 1980.

[52] *Cambridgeshire and Isle of Ely County Council* v. *Rust* [1972] 2 Q.B. 426 (English C.A.); *Dickens* v. *Gill* [1896] 2 Q.B. 310.

[53] *Wong Pooh Yin* v. *Public Prosecutor* [1955] A.C. 93 (P.C.).

[54] *Regina* v. *Wuyts* [1969] 2 Q.B. 474 (C.A.).

[55] *Cambridgeshire etc.* v. *Rust, supra*; *Regina* v. *Harvey* (1872), L.R. 1 C.C.R. 284.

(i) *Trespass at common law*

82. Unless a police officer can show affirmative justification either under a statutory authority, or at common law, entry upon private property will amount to a trespass at common law.[56] In *Eccles* v. *Bourque*[57] the Supreme Court of Canada recognized this principle while holding that there is a common law right permitting a police officer to enter premises by force if he has reasonable and probable grounds to believe that a person is on the premises whom he has authority to arrest.

83. Since Canadian Courts have not, as yet, gone very far in recognizing a tort protecting the individual's right of privacy as such, it is generally considered that, if no real damage is established, only nominal damages will be recoverable.[58] Yet it may not require much of an extension of the principles enunciated by the courts in awarding exemplary or punitive damages, to conceive that more than nominal damages could be awarded. The limitations placed upon awards of exemplary or punitive damages in a leading English case are that exemplary damages may be awarded only "where there has been oppressive, arbitrary or unconstitutional action by servants of the government".[59] The applicability in Canada of the limitations contained in the English case has been doubted by Mr. Justice Spence in the Supreme Court of Canada[60] and the case has specifically not been followed in at least four provinces.[61] Therefore it is possible that in Canada there will be a broader scope for exemplary damages.

84. Indeed, some Canadian cases have awarded exemplary damages in circumstances where no action of a "servant of the government" has been involved. In those cases the award has been made even when the defendant had no motive of personal benefit but was found to have committed "a deliberate trespass" or to have been "high handed" or to have shown "a contempt of the plaintiff's rights" or a "cynical disregard of the plaintiff's rights".[62] If these tests of awarding exemplary damages are the law in Canada, such awards might well be made against members of the R.C.M.P. who have made a surreptitious entry without lawful authority, particularly bearing in mind that senior members of the Force have known over the years that such entries

[56] *Ghani* v. *Jones* [1970] 1 Q.B. 693, per Lord Denning, M.R. at 706; Leigh, *Police Powers in England and Wales*, London, Butterworths, 1975, at pp. 167, 171 and 173.

[57] [1975] 2 S.C.R. 739.

[58] See, e.g., Burns, "The Law and Privacy: The Canadian Experience", (1976) *54 Can. Bar Rev.* 15.

[59] *Rookes* v. *Barnard* [1964] A.C. 1129 at 1226, per Lord Devlin.

[60] In his dissenting judgment in *McElroy* v. *Cowper-Smith and Woodman* [1967] S.C.R. 425 at 432.

[61] *Eagle Motors (1958) Ltd.* v. *Makaoff* (1970) 17 D.L.R. (2d) 222 (B.C.C.A.); *Fraser* v. *Wilson* (1969) 6 D.L.R. (3d) 531 (Man. Q.B.); *U.N.B.* v. *Strax* (1969) 1 N.B.R. (2d) 112 (N.B.S.C.); *Gouzenko* v. *Lefolii* [1967] 2 O.R. 262 (Ont. C.A.).

[62] *McKinnon* v. *F.W. Woolworth Co.* (1968) 70 D.L.R. (2d) 280 (Alta. App. Div.); *Turnbull* v. *Calgary Power Ltd.* [1975] 3 W.W.R. 354 (Alta. App. Div.); *Cash & Carry Cleaners* v. *Delmas* (1973) 7 N.B.R. (2d) 101; *Parkes* v. *Howard Johnson Restaurants* (1970) 74 W.W.R. 255 (B.C.S.C.).

amounted to trespass. On the other hand, as far as activities since July 1, 1974, are concerned, the possibility of such awards would exist only in the case of intelligence probes and not where an authorization has been given by a judge under section 178.13 of the Code or a warrant by the Solicitor General under section 16(2) of the Official Secrets Act, for in those cases the policeman entering the premises to install a listening device would have a genuine belief in his right to enter because the Department of Justice has given its opinion that he has such a right; and, even if (as we suggest in Chapter 3 of this Part) that is a mistaken view, such a genuine belief, even though mistaken, will preclude an award of exemplary damages.[63]

85. The ancient doctrine of trespass *ab initio*, which provides that a person who enters under authority but subsequently exceeds that authority may be treated as a trespasser from the time of initial entry, may be of some interest, particularly when initial entry is made pursuant to a judicial authorization under section 178 of the Criminal Code or a warrant under section 16 of the Official Secrets Act. It was clear from the evidence before us that members of the R.C.M.P. entering pursuant to such authorizations and warrants sometimes take the opportunity to search, and on occasion to copy or photograph material found — i.e. conduct an intelligence probe.

86. While the doctrine of trespass *ab initio* developed as a method of penalizing abuses of authority, its applicability has been doubted by commentators and courts in recent years, usually on the basis that it amounts to a penalty against honest police efforts or technical errors.

87. In addition the courts earlier developed the limitation that the doctrine is not applicable unless the abuse directly relates to the original ground and reason of entry. If this view is the law, then a partial abuse of authority does not render unlawful everything done under the authority.[64] Nevertheless some commentators, and *obiter dicta* in some Canadian cases, point out that since the rule was originally designed to provide a remedy against abuses of authority which might lead to oppression, it might still be useful for this purpose.[65]

(j) *Trespass under the Quebec Civil Code*

88. The relevant articles of the Quebec Civil Code are:

> 406. Ownership is the right of enjoying and of disposing of things in the most absolute manner, provided that no use be made of them which is prohibited by law or by regulation.

---

[63] *Cullerton* v. *Miller* (1894) 26 O.R. 36 (Ont. Q.B.D.).

[64] *Fleming, The Law of Torts* (5th ed., 1977) p. 101; *Salmond on Torts* (16th ed.) 1973, p. 48; *Elias* v. *Pasmore* [1934] 2 K.B. 164; *Canadian Pacific Wine Co.* v. *Tuley* [1921] 2 A.C. 417 (P.C.); *Chic Fashions* v. *Jones* [1968] 2 Q.B. 299.

[65] Denning, *Freedom under the Law*, p. 109; *Winfield & Jolowicz on Tort* (10th) 1975, p. 310; *Klar, Studies in Canadian Tort Law*, 1977, "Intentional Interference with Land", pp. 303-4; *Delta Holdings Ltd.* v. *Magrum* (1976) 59 D.L.R. (3d) 126; *Townesview Properties Ltd.* v. *Sun Construction* (1974) 56 D.L.R. (3d) 330 (Ont.).

1053. Every person capable of discerning right from wrong is responsible for the damage caused by his fault to another, whether by positive act, imprudence, neglect or want of skill.

89. Article 406 of the Civil Code describes in the most general terms the rights inherent in the ownership of property in the Province of Quebec. Trespass which may have been committed on such property, as a result of surreptitious entry performed by the R.C.M.P., may be considered a violation of the rights described in this article. Yet the Quebec courts have recognized trespass only in those circumstances where material damages have occurred as a result of such trespass. In those instances, damages have been awarded by the courts under article 1053 C.C. in order to compensate the owner of the property. The courts have refused to award exemplary damage for trespass and, as a result, where no material damage occurs, there can be no successful action for trespass.[66] It should be noted that any damage action for trespass under article 1053 C.C. is governed by a two-year limitation period pursuant to article 2261(2) C.C.

90. Some mention should also be made of the provisions of the Quebec Charter of Human Rights and Freedoms.[67] This legislation was enacted on June 28, 1976, and appears to cover some of the areas left unaffected by the Civil Code, including the right to sue for exemplary damages. Violations of this charter are brought before the "Commission des Droits de la Personne" which recommends the appropriate course of action before the courts. The manner in which the courts will acknowledge and protect the rights and freedoms protected by the Charter remains to be seen.

(k) *Conspiracy to commit trespass*

91. Section 423(2) of the Criminal Code provides as follows:

423. (2) Every one who conspires with any one

(a) to effect an unlawful purpose, or

(b) to effect a lawful purpose by unlawful means,

is guilty of an indictable offence and is liable to imprisonment for two years.

If two or more members of the R.C.M.P. conspire with each other to do an act which is trespass at common law, or which is an offence under a provincial Petty Trespass Act, does that constitute conspiracy "to effect an unlawful purpose"? If the act planned is an offence under a provincial statute, the offence of conspiracy is clearly established for the provincial offence is an "unlawful purpose".[68] Yet, even in that case, it may be possible to argue that

---

[66] *Cadorette et Autres* v. *Mlle Paris* [1951], B.R. 125; Nadeau, *Traité Pratiques de la Responsabilité Civile Délictuelle*, p. 188.

[67] L.Q. 1977, ch.C-12.

[68] *Wright, McDermott, Feeley* v. *The Queen* [1963] S.C.R. 539, [1964] 2 C.C.C. 201, 43 D.L.R. (2d) 597 (S.C.C.).

when the provincial offence is "trivial", section 423(2) should not apply.[69] In the case of an act which is simply trespass at common law, it is doubtful whether that is an "unlawful purpose" as that phrase is used in section 423(2). In *Grawelicz* v. *R.*[70] it was held that "in section 423(2(a) unlawful purpose means contrary to law, that is prohibited by federal or provincial legislation". Consequently in Canada it becomes unnecessary to consider whether conspiracy to commit common law trespass will be an offence only in limited circumstances, as had been held to be the case in England: *Kamara* v. *D.P.P.*[71] Presumably it is possible that those limitations might be applied in Canada to restrict liability for conspiracy to violate a provincial Petty Trespass Act. The limitations enunciated in *Kamara* v. *D.P.P.* were that conspiracy to trespass will amount to criminal conspiracy only when (a) something more than nominal damage is involved, or (b) where the public interest warrants criminal sanctions. It was held that the latter condition existed only when (i) premises were occupied to the exclusion of the rightful owner, and (ii) the action involved invasion of the public domain, for example by the occupation of a public building or (as in that case) the occupation of the embassy of a friendly power.

Legal and policy issues in C.I.B. work only

(a) *Surreptitious entries in drug investigation*

92. Surreptitious entries to search a place other than a dwelling-house may be made lawfully without a warrant only when the provisions of section 10(1) of the Narcotic Control Act are satisfied — i.e. when the peace officer

> reasonably believes there is a narcotic [in the place] by means or in respect of which an offence under this Act has been committed.

An identical provision in respect of controlled drugs is found in section 37(1) of the Food and Drug Act. These provisions do not enable unlimited warrantless search of a dwelling-house. Even with regard to a place other than a dwelling-house the policeman must "reasonably believe" there is a narcotic or controlled drug there; that is, he must have the belief, and it must be a reasonable one. This condition will not exist when the police have at most a suspicion that there is a narcotic or drug on the premises. Therefore a surreptitious entry and search where there is only such a suspicion would be a trespass, and might be an offence under the Criminal Code. (See the analysis of possible offences contained above, in section D, devoted to legal issues in respect of both the Security Service and the C.I.B..)

---

[69] *R.* v. *Layton, ex p. Thodas* [1970] 5 C.C.C. 260, 10 C.R.N.S. 290 (B.C.C.A.) per Nemetz, J.A. dissenting; M.R. Goode, *Criminal Conspiracy in Canada*, Toronto, Carswell, 1975, pp. 87-95; *R.* v. *Bendall* (1977) 36 C.C.C. (2d) 113, *R.* v. *Jean Talon Fashion Center Inc.* (1975) 56 D.L.R. (3d) 296 (Que. Q.B.) The latter case concerned an offence under a municipal bylaw. Whether a conspiracy to commit such an offence is now itself an offence is doubtful: see *Gralewicz* v. *R.*, discussed below at n. 65.

[70] (1981) 54 C.C.C. (2d) 289 (S.C.C.).

[71] [1973] 3 W.L.R. 198; [1973] 2 All E.R. 1242 (H.L.).

93. In addition, under both sections a peace officer, if he has the same reasonable belief, may enter and search a dwelling-house, but only if he has a writ of assistance. This is a general writ, issued pursuant to the Narcotic Control Act and the Food and Drug Act to a particular peace officer by a Federal Court judge, who must issue it when it is applied for by the Attorney General of Canada. (There has been much criticism of these writs, but as they are provided for by law we do not consider it to be within our terms of reference to comment on whether Canadian law should continue to permit them. Nor have we received any complaint that they have been used unlawfully by the R.C.M.P.) A covert search is lawful if it is made upon the authority of a peace officer who is in possession of such a writ and has a reasonable belief that there is in the place a narcotic or controlled drug by means or in respect of which an offence under the statute has been committed. Once again it must be emphasized that even if he has a writ of assistance, he cannot lawfully enter and search a dwelling-house unless he reasonably believes that a narcotic or a controlled drug is present there.

94. Finally, both sections provide that a justice may issue a warrant authorizing a peace officer to enter and search a dwelling-house, but the justice must be satisfied by information upon oath that there are reasonable grounds for believing that there is a narcotic or controlled drug present there.

95. The limitations on the powers of search found in these sections limit the ability of the R.C.M.P. in many circumstances to determine whether drugs are present. Consequently, as will be seen in section E of this Chapter, the R.C.M.P. want to have increased powers of search.

(b) *Surreptitious entries in investigations of "moonshining"*

96. The Excise Act, section 76(1), permits an officer, if he has a writ of assistance, to enter any building or other place to "search for, seize and secure any goods or other things liable to forfeiture under this Act". The word "officer" is defined as including a member of the R.C.M.P. The subsection reads in full as follows:

> 76. (1) Under authority of a writ of assistance, any officer, or any person employed for that purpose with the concurrence of the Governor in Council, expressed either by special order or appointment, or by general regulations, may enter in the night time, if accompanied by a peace officer, and in the day time without being so accompanied, any building or other place, and may search for, seize and secure any goods or things liable to forfeiture under this Act, and in case of necessity, may break open any entrance or other doors, walls, floors, windows or gates and any chests or other packages for that purpose.

On the face of the statute, no suspicion or belief in the existence of any particular set of facts need exist: there is no reference whatsoever to any such need. Yet in its brief to us the R.C.M.P. say that there may be surreptitious entry pursuant to section 76(1) only "when reasonable and probable grounds are sufficient to indicate that an offence is being committed". For this proposition an opinion by the Legal Branch is cited (Ex. E-1, Tab 4A), but that opinion does not relate to section 76(1). It discusses the search sections of the

Narcotic Control Act and the Food and Drugs Act, which do certainly require reasonable belief that a drug is present. Therefore the opinion does not support the view expressed in the brief. In our opinion section 76(1) does not contain any limitation, express or implied, as to a search being permissible only when there is a certain level of suspicion or belief in the existence of a state of facts. Consequently it is difficult to understand that any obstacle stands in the way of covert entry by an officer who possesses a writ of assistance.

(c) *Surreptitious entries in white-collar crime investigations*

97. The R.C.M.P. assert that in some cases surreptitious entry can be a valuable investigative technique in detecting "white-collar" crime. The example given was a case in which a covert search of a hotel room was made in the hope of gaining intelligence as to the intentions of a group of known "white-collar criminals" who were using the room but had left it temporarily. By chance, the search uncovered valuable stolen securities in the room. As a result, the R.C.M.P. called in the local police who later checked the suspects when they were leaving the hotel, and found the stolen securities. Convictions resulted. A search warrant could not have been obtained on mere suspicion. However, as far as the ability of the police to enter the hotel room is concerned, it is not clear that this case illustrates any limitation imposed upon the police by the law in the circumstances, for the policemen did not intend to commit an indictable offence and did not do so (hence there was no break and enter). Civil trespass did not occur because the law does not regard an ordinary short-term hotel guest as an "occupier" of his hotel room in the sense that he has a property interest sufficient to found an action for trespass. If the hotel manager gave permission for the entry, there was likely no trespass. In saying this we are speaking only of the entry into the room; any rummaging among personal effects may have constituted trespass to chattels (see Chapter 8 of this part).

E. NEED AND RECOMMENDATIONS — BRIEF SUMMARY

Security Service

98. We have already quoted extensively the explanation given publicly of the ways in which the Security Service finds that surreptitious entry for the purpose of intelligence probes is valuable in the investigation and detection of espionage, subversion and terrorism. Almost all the 47 cases that have been disclosed to us, mostly in summaries, and that were referred to in section C of this Chapter, involved targetted individuals who were suspected of espionage or foreign interference, or of links with terrorist groups. (Abridgments of many of these summaries are given as an Appendix to this Chapter.) Almost all these cases, and the one additional case which we mentioned, had an international element. There is no evidence that the Security Service has relied significantly upon surreptitious entry as a technique of investigation in cases where the suspected activity is believed to be purely domestic and where there is no suspicion of serious acts in terms that would justify application of the label "terrorist".

99. For reasons which we shall give in detail in Part V, Chapter 4, we consider that the need exists for the availability to the security intelligence agency, subject to external controls, of a limited lawful power of covert search where the investigation relates to suspected espionage, sabotage, foreign interference, or acts of political violence and terrorism which if carried out would cause grave injury to a person or serious damage to property. We do not come to this conclusion lightly, for we believe that any power to enter a man's house without his consent should be extended only with care.

C.I.B.

100. The R.C.M.P. has asserted, in a brief to us, that

> There is a definite, and often an essential, requirement to resort to this investigative technique when the manufacture of illicit drugs and alcohol comes under the scrutiny of resourceful investigators. Eventually a time comes when members employed on lengthy, difficult investigations, many of high security risk, are faced with the problem of having to know for sure
>
> — if an illicit drug laboratory or still is secreted in a place;
>
> — if the laboratory or still is producing or, is in the development stage;
>
> — if a cache of drugs or alcohol is in a place;
>
> — if quantities of illicit drugs or spirits are being removed from a cache bit-by-bit for trafficking purposes.

The Force considers that it is particularly difficult, without the power to search in circumstances when a search warrant could not be obtained, to detect the existence of clandestine drug laboratories. The difficulties lie in locating the hidden laboratory and identifying the persons involved. These persons are said to be frequently well financed, intelligent and particularly skillful in creating security measures to guard against discovery by police. It is contended that such persons are often acquainted with the law so that they know that they are relatively safe from prosecution until the last stage of manufacture, for until then they have not created a substance the manufacture or possession of which is prohibited under the schedules to the Narcotic Control Act and Food and Drugs Act that identify prohibited substances. In other words, they know that arrest and seizure are possible only at and after the moment the process results in the production of a prohibited substance. Frequently, we were told, they will move the clandestine laboratory to a new location for the final stage of production. At the least sign of interest by the police, the conspirators will close down the laboratory. Consequently the R.C.M.P. feel that only surreptitious entry, and the taking of samples and photographs during such entry, can enable investigators to determine whether and when the moment has arrived when arrest and seizure would produce evidence that would lead to a conviction and, with luck, will enable investigators to catch the major participants at the scene. The R.C.M.P. state: "In almost every case, seizure of a clandestine laboratory and arrests of persons involved are possible only by a program of surreptitious entry and examination." The R.C.M.P. assert also that surreptitious entry is essential in some investigations of trafficking in such narcotics as heroin and cocaine. They say that it enables the discovery of caches, the photography and marking of drugs for later identification, and determining

whether portions are being removed for distribution. Moreover, they say, this investigative technique permits the police to detect the identity of persons, often previously unknown, who are participants in the scheme.

101. The R.C.M.P. assert also that surreptitious entry is a valuable tool generally in the fight against "white-collar" crime. This has not been substantiated before us. True, in regard to "white collar" crime as in regard to many other kinds of crime, particularly crimes against property interests, the police forces would find it useful to be able to search undetected in offices and homes to try to find some evidence of the commission of a crime. However, we consider that any broad power to search private premises, even upon warrant duly issued, upon mere suspicion that there might be evidence there of the commission of an offence or the intended commission of an offence, would be contrary to the established traditions of criminal law enforcement procedure in Canada. If what was being sought were the power to search upon warrant granted upon suspicion, and the search was to be made known to the occupant at the time of the search or soon thereafter, at least the power to enter and inspect would have many counterparts in federal and provincial regulatory laws. However, what is sought by the R.C.M.P. is a power to search covertly. Such a power, we think, should be granted by statute only after a thorough review of all police powers of search and seizure, a review which should study this proposal in the context of the entire ambit of such powers. We therefore decline to make any recommendation in regard to this proposal.

APPENDIX

SECURITY SERVICE: SOME CASES OF SURREPTITIOUS ENTRY FOR THE PURPOSE OF INTELLIGENCE PROBES

Counter-espionage

(a) *Search of premises for paraphernalia and documents*

(i) Paraphernalia or documents found

1. A dwelling of a suspected illegal agent of a foreign intelligence service was searched for evidence of illegal activities. Some equipment suitable for intelligence purposes was found, and the investigation was continued by other means. Ultimately the suspect left Canada.

2. The Security Service searched the dwelling of a suspected intelligence officer of a foreign country to look for evidence of specific operations. Some equipment suitable for intelligence purposes was found. The individual was later identified as an agent of the foreign intelligence service.

3. Several entries were conducted into the residence of a Canadian suspected of being an intelligence agent for a foreign country. Important evidence of espionage was discovered.

4. More than one entry was made into the residence of a Canadian considered by the Security Service to be a foreign intelligence officer. Certain documents, considered to be of significance, were discovered and photographed.

(ii) Paraphernalia or documents not found

5. The Security Service searched the residence of a suspected illegal agent of a foreign intelligence service. The search failed to reveal any espionage paraphernalia. This contributed to an ultimate conclusion that the individual was not and had never been an agent of any intelligence service.

6. The Security Service searched the residence of a foreign mission employee who, the Service believed, was running Canadian agents. While no espionage paraphernalia was found, other useful information was obtained.

7. A search of the residence of a known foreign intelligence officer revealed no technical paraphernalia but did produce other useful information.

8. A Canadian was suspected by the Security Service of engaging in intelligence activities on behalf of a foreign power. His residence was searched, but no information of value was obtained. Other means of investigation led to refusal of re-entry to Canada of the employee of a foreign mission.

9. A search of a Canadian's residence produced partial substantiation of other evidence that dispelled suspicions that he had been recruited by a foreign intelligence agency.

10. On the basis of information received, business premises were searched in order to determine whether certain items were there being held for a person suspected of being a foreign agent. The search revealed no such information, but, during the search, photographs were taken of documents pertaining to the organization whose premises were searched.

(iii) To observe the lifestyle of an intelligence officer

11. A search of a residence produced what the Security Service considered to be information that increased their insight into certain aspects of a foreign country's intelligence service community.

(iv) To conduct a survey preparatory to installing listening device

12. Residential premises of a foreign mission employee, who was a suspected foreign intelligence officer, were entered to determine whether it would be possible to install a listening device and to locate certain things which would be of use in further investigation. After further investigation the mission employee was declared *persona non grata* and left Canada.

13. The residence of a Canadian, suspected of having been recruited by a foreign intelligence service, was searched in order to conduct a physical survey preparatory to introducing a listening device. While on the premises then and on a later occasion, Security Service personnel found no evidence to connect him with any intelligence operation. Further investigation satisfied the Security Service that he had no such connection.

Foreign interference

(i) Search of premises

14. A search of a residence produced no evidence that the occupant was, as suspected, a foreign intelligence agent. However, some information was found that was considered to be of use to Security Service work generally.

15. A search of a residence enabled letters to be photographed between the occupant, who was suspected of having been recruited by a foreign intelligence agency, and other persons.

(ii) Search of baggage

16. A suspected foreign intelligence agent's luggage was searched and a document of interest was photographed.

Possible terrorist group

(i) Search of premises

17. Office premises of a Canadian group, with objectives similar to those of a foreign violence-prone group, were searched, but the quality of information obtained was not significant.

18. Security Service personnel entered the office of a violence-prone group in which there was reason to suspect the presence of weapons. The purpose of the search was to look for weapons and for other information of interest. As a result of what was found, local police obtained a search warrant and some weapons were seized.

19. The Security Service searched the office of a group thought to pose a threat to security, in order to obtain details of the operation of the group and of its membership. Such information was obtained.

20. A search of an office enabled the Security Service to assess the capability of an organization in relation to international terrorism.

21. A Canadian resident's premises were searched to determine the extent of his ties with a foreign terrorist organization. No information of intelligence value was obtained.

22. Searches of a Canadian's residence produced useful information as to his relationship with terrorist groups in Canada and abroad, and plans for steps to follow assumption of power by the Canadian group.

23. A search of the office of an organization failed to produce the information which was sought, as to its finances.

24. A search of a residence produced no information of intelligence significance as to a person suspected of being linked to a foreign terrorist group.

(ii) Search of baggage

25. Security Service personnel searched luggage in transit, of a person suspected of carrying handguns, and found weapons.

26. A foreigner was believed to be shipping arms from Canada to his country. A search of luggage being sent by him out of Canada produced nothing of intelligence interest.

27. A foreign agency believed that one of its nationals in Canada had documents of interest, and asked that his luggage be searched. When carried out by the Security Service, some items of interest were found. It will be observed that in this case the activities of the Security Service were not directly related to any security interests of Canada.

CHAPTER 3

ELECTRONIC SURVEILLANCE — SECURITY SERVICE AND C.I.B.

A. ORIGINS, NATURE AND PURPOSE OF THE PRACTICE

1. The interception of telephonic messages has been technically possible since the early years of this century. In the United States, the constitutionality of the practice was argued before the Supreme Court in 1928[1] an indication of the rapidity with which law enforcement agencies recognized the potential worth of this technique. It has been used as an investigative technique by the R.C.M.P. since the 1930s. At the time counter-subversive functions were not performed by a branch separate from those in charge of criminal investigation, and there was nothing in the nature of counter-espionage being undertaken. Nevertheless, it was in what we would now regard as Security Service work that telephone tapping was begun in the latter part of that decade. In the years following the Second World War both telephone tapping and eavesdropping by means of microphones became more common among Canadian police forces. Telephones could be tapped by the installation of equipment along the telephone lines or at the telephone company's exchange. Later, telephone conversations could be listened to by means of induction devices installed in the telephone receiver; these were essentially the same for functional purposes as microphone "bugs" transmitting by radios which, with technical advances, could be installed more readily than the earlier microphones that transmitted by wire.

2. All these forms of eavesdropping devices were found to be valuable investigative techniques, both in the detection and investigation of crime and in the work of the Security Service. The increasing use of the technique by police forces received relatively little public attention in Canada. For the R.C.M.P. at least, telephone tapping was regarded as risky because it might involve violations of various statutes, and, to the extent that it was used at all, it was therefore regarded as an investigative aid to be employed in support of other techniques so that it would not have to be disclosed in court. Eavesdropping by microphone, so far as we can tell, was probably used more in Security Service

[1] (1928) 277 U.S.438.

functions (where the principal object is not the collection of evidence for the purpose of prosecution) than in criminal investigation, and in any event disclosure of its use in particular cases of criminal investigation would not have been regarded as a good idea because to do so would have alerted criminals and other adversaries to the techniques of installation and, in the particular case, might have exposed co-operating persons such as hotel employees and informers within criminal or subversive groups to the possibility of retaliation.

Criminal investigation

3. The value of telephone tapping in criminal investigation was testified to before us by Assistant Commissioner T.S. Venner, who, in 1973 became officer in charge of criminal intelligence for "O" Division (Southwestern Ontario):

> . . . when I came to "O" Division it was immediately apparent that, number one, it was virtually impossible to do effective criminal investigation in the City of Toronto, or in that general area, without telephone tapping on the criminal side. The difficulties that were presented by refraining from this activity were such that we were just almost out of business.
>
> (Vol. 33, p. 5440.)

The Annual Reports submitted by the Solicitor General of Canada reveal that in a significant number of criminal proceedings, evidence has been gathered from private communications intercepted pursuant to a judicial authorization issued under section 178.13(1) of the Criminal Code, and that a number of convictions have resulted. In numerous other cases information obtained from interceptions was used in the investigations though it was not offered in evidence.

	Cited as Evidence	"Used" but not in evidence	Convictions
1974 (half-year)	101	155	83
1975	395	879	246
1976	284	787	148
1977	198	546	134
1978	172	550	105
1979	101	155	83

This information is based on R.C.M.P. investigations, principally of offences under the Narcotic Control Act and the Food and Drugs Act, and conspiracy under the Criminal Code (most of which would no doubt be narcotic and drug cases).

4. The Annual Report for 1979, in its "General Assessment", disclosed the following statistics as to the first five years of the operation of the Protection of Privacy Act:[2]

	1974	1975	1976	1977	1978	1979
Authorizations granted	140(1)	562	613	615	712	764
Number of persons arrested	344	1561	1499	1213	1381	1177(2)
Number of convictions	238(3)	1125(3)	945(3)	680(3)	655(3)	225(3)
Authorization/Arrest ratio	2.5(4)	3.6(4)	2.5(4)	2.0(4)	1.9(4)	(6)
Arrest/Conviction ratio	69.2(5)	72.1(5)	63.0(5)	56.1(5)	47.4(5)	(6)

(1) Act in force for six months only in 1974.
(2) Other arrests pending.
(3) Cases are still before the courts in relation to investigations of authorizations originating in 1974 through to 1979.
(4) &(5) These ratios will increase as investigations and prosecutions are completed.
(6) No meaningful ratios available at this time.

Using 1975 as an example, the 1979 Annual Report showed that, allowing for the lapse in many cases of from one to at least four years between the granting of an authorization and arrests and convictions in the cases concerned, the figures originally reported in the year of the authorization undervalued the significance of electronic surveillance as an investigative technique. There were 562 authorizations in 1975. In those cases the following arrests and convictions ultimately occurred:

Results of 1975 Authorizations

	Number of Arrests	Number of Convictions
Figures reported in 1975	1,208	196
Figures amended in 1976	1,492	514
Figures amended in 1977	1,523	836
Figures amended in 1978	1,557	968
Figures amended in 1979	1,561	1,125

The Annual Report stated that at the end of 1979 there were still some cases concerning authorizations obtained in 1975 before the courts, so that the number of convictions is expected to increase slightly in 1980. This delay should be borne in mind in considering the apparently low number of cases in which evidence was adduced and convictions obtained in cases in which the

[2] The fourth and fifth categories of the table appear to be described incorrectly: the fourth category should be "Arrest/authorization ratio", and the fifth category should be "Conviction/arrest" and is, it should be observed, not a ratio but a percentage.

authorizations were granted in the years 1976 to 1979: the full story of the number of convictions obtained in those cases is not yet known.

5. It is important to note that the statistics shown here relate to applications for authorizations made by agents of the Solicitor General of Canada, and do not include any information concerning applications made by agents of provincial attorneys general. The latter would cover the majority of investigations under the Criminal Code. Thus, for example, the Annual Report of the Attorney General of Ontario for 1978 disclosed that in that year in Ontario there had been 237 applications for authorizations for wiretapping. In 1978 these applications in Ontario covered the following offences:

	Suspected Substantive Offence	Suspected Conspiracy to Commit the Offence
Bookmaking	61	45
Theft, robbery and breaking and entering to commit theft	52	47
Possession of stolen property	41	36
Fraud	32	31
Murder	26	18
Extortion	20	19
Possession of counterfeit money	10	0
Forcible confinement	5	0

Although those figures are not related to investigations conducted by the R.C.M.P., the overall purpose of electronic surveillance cannot be understood without reference to the provincial scene. Of particular interest is the fact that the 1978 Annual Report of the Ontario Attorney General disclosed that 76 transmitting devices were installed. Although no precise information is available, it may reasonably be inferred that a number of such microphone installations by police forces other than the R.C.M.P. have been made by entry without the consent of the person entitled to give permission to enter the premises. Thus the legal problems in Chapter 2 of this Part are not limited to the work of the R.C.M.P.

Security Service

6. From July 1, 1974, to the present, most warrants signed by the Solicitor General have been signed by him at his regular weekly meetings with the Director General. The totals of warrants issued from 1974 to 1978 inclusive have been stated in the Annual Reports made by the Solicitor General to Parliament pursuant to section 16(5) of the Official Secrets Act, as follows:

1974 — 339
1975 — 465
1976 — 517
1977 — 471
1978 — 392
1979 — 299

7. The annual figures are somewhat misleading because they include renewals which, in December of each year from 1974 to 1978, were signed by the Solicitor General to authorize continuation, from the first day of the following January until the 31st day of the next December, of the interception of communications under warrants already signed. This procedure is not provided for by the statute. It resulted from an administrative decision made within the Security Service that all warrants should be issued for periods no greater than the period ending December 31 of the year in which the warrants are issued. This decision was made by the Security Service with good intentions, as it was thought that otherwise the statistics provided to Parliament would be misleading in that, if a warrant were granted for a period expiring in the following year, the annual report to Parliament would not in fact disclose the total number of warrants which were in effect in that year. However, it does not seem to have been realized that the new system led inadvertently to another misinterpretation.

8. There is no provision in section 16 of the Official Secrets Act for renewals of warrants. By way of contrast, section 178.13(3) of the Criminal Code expressly provides that a judge may grant "renewals of an authorization" from time to time. The Honourable Allan Lawrence, Solicitor General in December 1979, did not follow the procedure which his predecessors had followed. Perhaps this was because the issue of the validity of the granting of renewals had been raised with Mr. Allmand during the latter's *in camera* testimony on December 3, 1979, later made public in Vol. 162 (March 7, 1980). The procedure followed by Mr. Lawrence was to receive applications for new warrants only.

9. The renewal procedure and its effect on the statistics are exemplified by the fact that on December 20, 1974, Mr. Allmand signed a document purporting to renew 222 warrants previously granted by him. The number of warrants reported in the Annual Report for 1975 as having been issued in 1975 included the 222 renewals. The same was true in following years. Thus in December 1975, there were 214 renewals, of which 128 were renewals of warrants which had originally been granted in 1974 and renewed in December 1974. On December 20, 1976, 199 renewals were granted, of which 97 referred to warrants originally granted in 1974 and renewed at the end of both 1974 and 1975, and 28 referred to warrants which had been issued in 1975 and renewed at the end of 1975.

10. It should not be assumed that the Solicitors General have acted as rubber stamps upon receipt of applications for warrants. Eleven applications made to the various Solicitors General from 1974 to 1978 inclusive were refused. One Solicitor General rejected three applications but subsequently granted them when more information, especially as to the likelihood of the usefulness of the warrant, was provided to him. Another rejected three applications, one because it was proposed to be used to intercept the communications of a person on a university campus, a second for a reason that was not recorded by the Security Service, and a third for the reason, as reported on Security Service files, that he knew one of the people in the suspect group and was sure that that person was doing nothing illegal. (That former Minister, however, has told us that he remembers the application and that that is not what he said. He says that he

did not know the person but had heard of him, and that he did not say he was sure that the person was doing nothing illegal. What he did say, according to the Minister, is that he needed better evidence that the group fell within the statutory provisions.) Another Solicitor General rejected five applications. One of these applications had been made on the ground that the target was said to be a member of a foreign terrorist group and who had participated in a bank robbery in his native country in an attempt to collect funds for the terrorist group. In one instance the Solicitor General rejected the application because he required more information that the person was involved in the terrorist field "in Canada". Later in this chapter we shall comment on whether the statute requires such proof; our point here is simply that the Solicitor General did not grant the warrant sought.

11. The previous paragraph affords substantial evidence that the Solicitors General did not always comply with the wishes of the Security Service as expressed in applications made under section 16(2). In this regard the following points should also be noted. Three warrants, which had been issued and acted upon were subsequently terminated by the Solicitor General contrary to the wishes of the Security Service. Three warrants issued by the Solicitor General were for a shorter period than the Security Service had requested, and were not renewed at the expiry of the period. Finally, on one occasion, a Solicitor General, in a special review requested by him of 22 warrants, cancelled six of them, as in his opinion their continuation was not justified.

B. R.C.M.P. POLICIES CONCERNING THE PRACTICE

Criminal Investigation Branch

12. In those parts of Canada served by the Bell Telephone Company, it was an offence, even before July 1974 when wiretapping was not covered in the Criminal Code, to intercept wilfully any message transmitted on the company's telephone lines. Section 25 of the Act incorporating the Bell Telephone Company of Canada reads as follows:

> 25. Any person who shall wilfully or maliciously injure, molest or destroy any of the lines, posts or other material or property of the company or in any way wilfully obstruct or interfere with the working of the said telephone lines or intercept any message transmitted thereon shall be guilty of a misdemeanour.[3]

13. This section does not appear to have been interpreted in any court until the decision in *Re Copeland and Adamson* in 1972. Mr. Justice Grant held that telephone tapping was not a violation of the section:

> The only part of such section which it might be said would be breached by wire-tapping would be the words "interfere" or "intercept". Can it be said that listening in on a telephone conversation is properly described by either of such terms? The Shorter Oxford English Dictionary defines the word "interfere" as follows:
>
> "To interpose — intersperse; to strike against each other; to come into collision; to exercise reciprocal action so as to increase, diminish or nullify the natural effects of each."

[3] S.C. 1880, ch.67, s.25.

It defines the word "intercept" as follows:

> "To take or seize by the way or before arrival at a destined place; to stop or interrupt the progress or course of; to interrupt communications or connections with."
>
> I do not believe that wire-tapping which does not impede the conversation between the parties nor impede its progress can form a breach of such section because the material before me does not indicate that the audio surveillance creates any disturbance of the conversation.[4]

The same point of view was expressed by a brief on wire-tapping prepared in 1965, apparently by the Legal Branch of the R.C.M.P., which pointed out that the phrase "intercept any message", in the absence of judicial interpretation, "must take its everyday meaning, i.e. to take or seize on the way from one place to another, cut off, check, stop — in other words so that the message would not be received by the intended receiver." However, it may be assumed from what follows that, before *Re Copeland and Adamson* was decided, at least some people thought that the word "intercept" included listening. (It may be noted that section 178 of the Criminal Code, which came into effect on July 1, 1974, has specifically avoided the difficulty by defining "intercept" as including "listen to, record or acquire a communication or acquire the substance, meaning or purport thereof".)

14. In two provinces, Alberta and Manitoba, legislation specifically prohibited the interception and clandestine recording of telephone messages by any means, including induction, as Commissioner McClellan noted in a letter to the Deputy Minister of Justice in 1965. The Commissioner, probably relying on the legal brief, did not mention the provision in the Bell Telephone Act in his letter. He wrote that

> . . . with the exception of the Provinces of Manitoba and Alberta, there is no legislation in force primarily enacted to prohibit telephone intrusion.

He expressed his "belief that a law enforcement agency is not prohibited from intercepting telephone conversations". (Ex. E-1, Tab 21).

15. In 1936 it appears that Assistant Commissioner G.L. Jennings, who was Director of Criminal Investigation, consulted the Deputy Minister of Justice with regard to wiretapping. A member of the Department prepared a memorandum of which a copy was then sent by the Deputy Minister to Assistant Commissioner Jennings. The memorandum quoted section 25 of the Bell Telephone Act, then, clearly assuming the practice to be illegal, cited three Canadian judicial decisions that evidence is admissible in court even if obtained illegally. Assistant Commissioner Jennings in his acknowledgement to the Deputy Minister, described the memorandum as including "legal opinions on the admissibility of evidence obtained in an irregular manner" and advised that the information had been disseminated throughout the Force. In his letter to the officers commanding the various divisions the Assistant Commissioner observed that it might be necessary to resort more and more to wiretapping, and that "the consensus of the legal opinion" is that evidence obtained "in an

[4] [1972] 3 O.R.248, 28 D.L.R. (3d) 26.

irregular manner" is admissible and that it is "not material to the case in what manner such evidence was obtained". (Ex. E-1, Tab 1A.)

16. Thus R.C.M.P. Headquarters encouraged the use in some of its Divisions of a technique that was then thought to be an offence under the Bell Telephone Act. Presumably wiretapping was used in criminal investigations at least until 1959, for in March of that year a memorandum by Inspector (later Commissioner) Higgitt recorded that Commissioner Nicholson had "forbidden the use of technical aids equipment for the interception of telephone conversations". (Ex. E-1, Tab 1B.)

17. From that time onward there is considerable evidence (Ex. E-1, Tab 2) that senior officers at Headquarters, including Commissioner Lindsay in 1967 and three Directors of Criminal Investigation in 1964, 1966 and 1969, reiterated the policy forbidding the use of telephone tapping by members of the Force in the investigation of criminal matters. Indeed, in 1966 Commissioner McClellan, in a letter, assured the Solicitor General, the Honourable L.T. Pennell, "that this Force does not practise telephone tapping in the investigation of criminal matters". (Ex. E-1, Tab 2K.) At a meeting on July 5, 1968, according to a memorandum prepared by Commissioner Lindsay, he and other senior officers advised the Solicitor General, the Honourable John N. Turner, of "the total absence of wiretapping by us in this field" (i.e. in criminal investigations). A note from Commissioner Lindsay records that the same matter was discussed "in general terms" on July 11, 1968, with the newly appointed Solicitor General, the Honourable George McIlraith. An exception was made in cases where the consent of one of the parties to the conversation was obtained. At the time the listening and recording of a conversation with the consent of one of the parties was done by using an induction device near but not necessarily attached to the party's telephone or wire. Even this technique was not permitted in Alberta and Manitoba, because of local legislation (Vol. 33, pp. 5430-1). This technique might have been a violation of section 25 of the Bell Telephone Act, but the practice was known in the courts and even by Chief Justice Dorion (in the Inquiry into the Munsinger affair in 1965) without raising adverse comment. Nevertheless, these senior R.C.M.P. officers wanted the use of this investigative aid to be kept out of the public eye as much as possible, particularly as they had hopes of obtaining legislation that would permit the use of wiretapping by warrant, and they feared that public exposure might prejudice the enactment of the legislation. Although the Force's policy forbade participation in joint operations with other Canadian police forces in the interception of telephone messages or in manning listening posts, there was no hesitation in using the product of such activities or transcribing tapes. In fact, the prohibition of telephone taps by Headquarters was seen by the Force to cause tensions with other police forces, most of which conducted telephone tapping (Vol. 33, pp. 5395 and 5400).

18. Therefore, so far as can now be ascertained, and so far as practice reflected Headquarters policy, the use by the R.C.M.P. of devices to intercept telephone conversations, at least from 1959, was limited to the use of induction devices with the consent of one party to the conversation. According to *Re Copeland and Adamson*, however, this was not an offence.

19. It is clear that the policy enunciated by Headquarters, and the assurances given so positively to government that telephonic interception was not permitted, were somewhat meaningless. Assistant Commissioner T.S. Venner testified that in "some areas" R.C.M.P. investigators "simply relied on their local, municipal and provincial police counterparts to do this work for them". In other areas,

> ... our policy was held to be just a guideline, and key personnel, when operational circumstances warranted it, went ahead with the necessary activity, either not reporting it at all, reporting it only up to certain levels or reporting it in an incomplete, less than fully informative fashion.
>
> (Vol. 33, p. 5404.)

One such area was "O" Division (Southwestern Ontario), to which Mr. Venner was transferred from Edmonton in the summer of 1973. Put more bluntly by him, the fact that telephone tapping was being carried on in the field was "withheld" from senior officers of the Force who were responsible for the policy and were assuring Parliamentary Committees that there was no wiretapping for criminal investigation purposes (Vol. 33, p. 5453). Indeed, in those areas where the policy was ignored in practice, the R.C.M.P. now recognizes that the telephone tapping was "carried on in an atmosphere of non-accountability, fear of discovery, even deception" (Vol. 33, p. 5407).

20. Mr. Venner told us that when he moved from Alberta to Toronto in 1973 as Officer in Charge of the Criminal Intelligence Division

> It also became apparent that telephone tapping was going on, was being conducted by our criminal investigators, and to a very high degree it also became apparent that this was an underground activity, that it was not being reported, that information as to the character and extent of our technical activity was being withheld from superior officers, and the people who were doing it were people who became immediately subordinate to me as soon as I arrived there.
>
> (Vol. 33, p. 5440.)

So, after examining the situation, he concluded that it was "impractical" not to tap telephones, "policy notwithstanding". Although it was "clear" to Assistant Commissioner Venner that in 1973 "it was still a policy of the Force not to wiretap" (Vol. 33, p. 5454), he considered the policy to be

> ... a guideline to be followed wherever possible, but when it was just not practical to live within that policy, and where there was a greater public interest, in my assessment, at stake, then telephone intrusion would form part of our electronic surveillance program.
>
> (Vol. 33, p. 5441.)

He was aware not only that the practice was contrary to Force policy, but that, in the small percentage of cases in which it was necessary to enter premises in order to tap a telephone, there was ("at most") a violation of the Ontario Petty Trespass Act and possibly civil trespass (Vol. 33, pp. 5441-44).

21. This attitude was not restricted to Southwestern Ontario. In a letter to the Solicitor General on October 6, 1977, Commissioner Simmonds wrote

> Efforts to have our policy changed met with no success for a variety of reasons and it became evident that there was a wide range of interpretation

being applied with respect to the prohibition against telephone tapping. In some areas, our investigators simply relied on their local, municipal and provincial police counterparts to do this work for them. In other areas, our policy was held to be just a guideline, and, key personnel, when operational circumstances warranted it, went ahead with the necessary activity either not reporting it at all, reporting it only up to certain levels or reporting it in an incomplete, less than fully informative fashion. In some other areas, the policy was rigidly adhered to, occasionally because local enforcement programs were sufficient without this investigative aid, but more often because the policy and public pronouncements by the Commissioners where held to be an absolute bar to telephone tapping in the investigation of criminal matters. I think it is fair to say that where this interpretation existed and was applied, telephone tapping simply continued in an "underground" fashion and our previously high standards of accountability became subject to violation. The damage this did has not yet been fully repaired.

(Ex. E-1, Tab 1.)

22. The self-imposed limitation was removed with the enactment of the Protection of Privacy Act, which came into effect on July 1, 1974. At least as far as the R.C.M.P. was concerned, that Act has apparently vastly increased the use of telephone intercepts for criminal investigation purposes.

Security Service

23. The R.C.M.P. Security Service has been intercepting telephonic communications since arrangements were completed for that purpose in 1951, under the Emergency Powers Act, which empowered the Minister of Justice to require a communications agency to produce or make available, any communication "that may be prejudicial to or may be used for purposes that are prejudicial to the security or defence of Canada". Superintendent George McClellan, who was then officer in charge of Special Branch, expressed the view, in a memorandum for the Honourable L.B. Pearson, that there was no legislation barring such action. However, the Minister of Justice, the Honourable Stuart Garson, appears to have been of a different view in January 1951 and a special procedure was apparently adopted to resolve the problem.

24. The Emergency Powers Act expired on May 31, 1954. That month the R.C.M.P. proposed that sections 3 and 11(1) of the Official Secrets Act could provide a satisfactory authority for continuation of interceptions of telephone communications after that date. On June 16, 1954, the Deputy Minister of Justice, Mr. F.P. Varcoe, gave a written opinion to the Minister of Justice, which for the next 20 years was known as "the Varcoe opinion" and was the rationale for the interception of telephonic communications for security purposes. His opinion was that telephonic communications could be intercepted pursuant to a search warrant granted by a justice of the peace under section 11(1) of the Official Secrets Act.

25. At the date of that opinion the relevant provisions of the Official Secrets Act[5] were as follows:

> 3. (1) Every person who, for any purpose prejudicial to the safety or interests of the State, (c)... communicates to any other person any... in-

[5] R.S.C. 1952, ch.198.

formation that is calculated to be or might be or is intended to be directly or indirectly useful to a foreign power; is guilty of an offence under this Act.

11.(1) If a justice of the peace is satisfied by information on oath that there is reasonable ground for suspecting that an offence under this Act has been or is about to be committed, he may grant a search warrant authorizing any constable named therein, to enter at any time any premises or place named in the warrant, if necessary by force, and to search the premises or place and every person found therein, and to seize any sketch, plan, model, article, note or document, or anything that is evidence of an offence under this Act having been or being about to be committed, that he may find on the premises or place or on any such person, and with regard to or in connection with which he has reasonable ground for suspecting that an offence under this Act has been or is about to be committed.

The reasoning, in part, was that while the search warrant provision in the Criminal Code is open to the possible construction that it relates only to tangible evidence, section 11 of the Official Secrets Act extends to "anything that is evidence of an offence under this Act". This "anything" must include oral communications, since the communication of information of the kind referred to in section 3, and in the circumstances referred to in that section, constitutes an offence, and Parliament must be presumed, in enacting section 11, to have had in mind every means of communication, including telephonic communication. Mr. Varcoe recommended a form of search warrant that was to be granted by a justice of the peace, reading as follows:

OFFICIAL SECRETS ACT

WARRANT TO SEARCH

Canada,
Province of ,
City of ,

To.....of the Royal Canadian Mounted Police in the said City of .....

WHEREAS it appears on the oath of..... that there are reasonable grounds for suspecting that an offence under the Official Secrets Act has been or is about to be committed, to wit: that information that is calculated to be, might be, or is intended to be, directly or indirectly useful to a foreign power concerning secret official code words, pass words, sketches, plans, models, articles, notes or other documents, prohibited places or things in prohibited places, or concerning things made or obtained in contravention of the Official Secrets Act, has been or is about to be published, communicated or transmitted by means of the telephone installed in .....

(here describe location of phone i.e. "house bearing civic number-..... street"
or
"apartment (or suite) no..... in the building bearing civic number-..... street" but do not use word "premises")

to agents of foreign powers and to other persons not lawfully entitled to receive such information, for purposes prejudicial to the safety or interests of the State; and that there are reasonable grounds for suspecting that evidence or communications that are evidence of an offence under the Official Secrets Act having been or about to be committed, by the communication, publication or transmission of such information by means of the said telephone, may be found in the premises of . . . . (hereinafter called the premises);

This is therefore to authorize and require you to enter into the said premises at any time and to search for, seize and record any communication or communications transmitted by means of said telephone installed in . . . . that is or are evidence of an offence under the Official Secrets Act having been or being about to be committed and with regard to or in connection with which you have reasonable ground for suspecting that an offence under the said Act has been or is about to be committed.

Dated this . . . . day of . . . . A.D., 195...

.....

Justice of the Peace in

and for . . . .

The intention of the R.C.M.P. in suggesting this procedure was to rely on section 17(1) and (2) of the R.C.M.P. Act which makes the Commissioner and every Deputy Commissioner, Assistant Commissioner, Chief Superintendent and Superintendent *ex officio* a justice of the peace. This procedure was in fact followed from 1954 onward. However, ten years later, the Minister of Justice, the Honourable Guy Favreau, by letter dated September 4, 1964, imposed a control mechanism which required the Commissioner to seek the authorization of the Minister in writing before the Commissioner (acting as a justice of the peace) would issue such a search warrant. The Commissioner was to make a written request for such authority to the Minister, who was to be satisfied "that such facilities are being or are likely to be used by a person engaged in, or reasonably suspected by the Commissioner of being engaged in or about to engage in activities which constitute offences made under the Official Secrets Act". There was an emergency provision for the Commissioner to issue a warrant for 72 hours. The Minister was to carry out a monthly review of all outstanding search warrants and he might re-authorize those which, in his opinion, there were sufficient grounds to retain. The interception of telegraphic communications was, as previously, to be based on an Order of the Minister of Justice under the authority of section 7 of the Official Secrets Act.

26. It was on the basis of the "Favreau letter" that the Ministers responsible for the R.C.M.P., until June 1974 received and approved monthly "certificates of review" for all current warrants for the interception of telephonic communications.

27. It should be noted that this procedure did not cover the interception of oral communications by microphone. The reason for the procedure in respect of telephonic communications was that the telephone companies wanted a legal

basis for the co-operation they were being asked to extend. No such concern inhibited microphone operations.

28. The Security Service policies concerning electronic surveillance by "bugging" — i.e. microphone installations — have been reviewed in Chapter 2, section B, because the legal issues arising from that practice relate to "Surreptitious Entries" and were best discussed under that heading.

29. Two examples might be useful in illustrating that the Security Service at Headquarters has exercised some prudence in deciding whether to apply for warrants. In one instance, the person whose communications were the subject of a proposed application for a warrant was an executive member of an organization about which Headquarters decided not to make application because the activities were not considered to be subversive. In the other instance, the targetted group had its origins in another country and a history of terrorist acts in Canada and other countries. While an earlier warrant had been granted against members of the group in Canada, a subsequent request by the field unit that a warrant be applied for in respect of the communications of a person believed to be the leader of the group in Canada was turned down by Headquarters because Headquarters had learned that the reason for the group's violent activities had ceased to exist.

C. EXTENT AND PREVALENCE — SECURITY SERVICE AND C.I.B.

(i) *Security Service*

30. Before July 1, 1974, as has already been indicated, "wiretapping" (which includes the interception of both telephone conversations and telex messages) was a common and frequently used investigative technique throughout Canada — and consequently in those provinces where it may have been an offence. The use of microphone installations, which *per se* was not unlawful but gave rise to legal issues in regard to the *manner* of their installation, use and removal, was also general and frequent.

31. Since July 1, 1974, the legal issues in regard to both wiretapping and microphone installations have changed. The use of both techniques remains general and frequent, and is disclosed in the Annual Reports of the Solicitor General.

(ii) *Criminal Investigation Branch*

32. We have already described the official refusal of the Force to permit the use of telephone tapping before July 1, 1974, and we have described what evidence we have obtained of the policy being disregarded at the local level. The evidence tended to refer to telephone tapping, and there is no evidence before us as to the use of microphones, but the extensive use of the latter since July 1, 1974, would lead us to infer that the evidence we received, which was expressed in terms of telephone tapping, applied equally to other forms of electronic surveillance.

33. Since July 1, 1974, the extent to which those techniques are used by the R.C.M.P. and other police forces has been disclosed in the Annual Reports of the Solicitor General of Canada and the attorneys general of the provinces which have been referred to in section A of this Chapter. They are used very extensively in the investigation of crime.

D. LEGAL AND POLICY ISSUES

(a) *Legal issues common to Security Service and C.I.B.*

Violations of Provincial Statutes

34. We have already described the most significant legal issue regarding telephone tapping before July 1, 1974. That issue was whether it constituted an offence under section 25 of the Bell Telephone Act. In *Re Copeland and Adamson* it was held not to be an offence under that Act unless the conversation was disturbed by the eavesdropping. Legislation in certain provinces also requires consideration in deciding whether telephone tapping before July 1, 1974, constituted an offence. The Alberta Government Telephone Act[6] makes it an offence to interfere with the provincial equipment or facilities, record conversations without advising the other party in advance and to use profane and other specified language on a telephone or telecommunication wire. The Manitoba Telephone Act[7] deals with the connection of receiving and transmitting equipment to provincial facilities without the approval of the Provincial Commission. The Act also prohibits the recording of telephone conversations in Manitoba unless the other party to the conversation is properly advised of the proposed recording. The Nova Scotia Rural Telephone Act[8] provides penalties for wilful and malicious interference with provincial telephone company equipment. The Quebec Telegraph and Telephone Companies Act[9] prohibits the use of provincial equipment to acquire, without lawful authority, knowledge of private conversations.

35. The Telephone Act of Ontario[10] prohibits interference with equipment and the divulging of telephone conversations to persons who were not parties to a conversation except when lawfully authorized or directed to do so. The Ontario Legislation was held to be *intra vires* the province: *R.* v. *Chapman and Grange.*[11] These provincial legislative provisions under which offences may, at least before July 1, 1974, have been committed by members of the R.C.M.P. engaged in the investigation of crime, do not appear to have been considered at any time within the R.C.M.P. when deciding upon the policy in regard to telephone tapping.

---

[6] R.S.A. 1970, ch.12.
[7] R.S.M. 1970, ch.T-40 as amended by 1977 Man., ch.45.
[8] R.S.N.S. 1963, ch.273.
[9] R.S.Q. 1964, ch.286.
[10] R.S.O. 1970, ch.457.
[11] [1973] 2 O.R. 290.

36. These provincial statutes continue in effect. However, it is likely, in our view, that the entry of the Parliament of Canada into the field by the enactment of the Protection of Privacy Act means that the provincial legislative provisions are no longer effective in so far as they are in respect of the same forms of conduct as are covered by the criminal legislation. Therefore it is likely that, since July 1, 1974, when members of the R.C.M.P. have tapped telephones under an authorization by a judge under section 178 of the Criminal Code or by the Solicitor General under section 16 of the Official Secrets Act there has been no offence committed under provincial legislation.

37. As for the Security Service, the position since 1974 has just been referred to. Before July 1, 1974, the tapping of telephones was carried out pursuant to warrants issued under section 11 of the Official Secrets Act. Consequently it is unlikely that offences were committed under the provincial statutes.

38. Listening to telephone communications in British Columbia and Saskatchewan (which do not have statutes creating offences specifically in regard to telephones) and *all* forms of electronic surveillance in those provinces as well as Manitoba may violate the provisions of the Privacy Acts of those provinces.[12] These statutes create "a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of another".[13] With minor differences the three provincial statutes very closely resemble each other. All three provide that privacy may be violated by eavesdropping or surveillance whether or not accomplished by trespass. However, they all provide certain defences to such actions, one of which is particularly pertinent. As stated in the Saskatchewan Act (and similarly in the statutes of the other provinces):

> 4. (1) An act, conduct or publication is not a violation of privacy where:
>
> (a) it is consented to, either expressly or impliedly by some person entitled to consent thereto;
>
> ...
>
> (c) it was authorized or required by or under a law in force in the province or by a court or any process of a court; or
>
> (d) it was that of:
>
> (i) a peace officer acting in the course and within the scope of his duty; or
>
> (ii) a public officer engaged in an investigation in the course and within the scope of his duty;
>
> and was neither disproportionate to the gravity of the matter subject to investigation nor committed in the course of trespass.

In the case of defences for peace and public officers the Acts seem to set up a series of variable permissible violations of privacy directly proportionate to the seriousness of the "crime".

---

[12] Stats. B.C. 1968, c.39; Stats. Saskatchewan 1973-74, ch.80; Stats. Manitoba 1970, ch.74.

[13] Privacy Act, Stats. B.C. 1968, ch.39, s.2(1).

39. However, if a policeman cannot be said to be carrying out his duty if he violates some other law, such as the law of trespass, the general applicability of a defence under section 4(d) must be discounted in cases of surreptitious entry. On the other hand authorizations or warrants issued since July 1, 1974, under section 178 of the Criminal Code or section 16 of the Official Secrets Act would mean that most otherwise actionable incidents involving members of the R.C.M.P. would be covered by a defence under section 4(c).

40. We turn now to a consideration of a number of legal issues which are common to both sides of the Force and pertain to the period from July 1, 1974, to the present time.

Entry into private premises

41. The first issue to be considered is whether a judge or a Solicitor General, in issuing a warrant, has the statutory power to authorize entries to install, repair and remove a listening device, and whether if he does not expressly do so, the power is implied. During the early months of 1972, while consideration was being given in government to the Protection of Privacy Bill, the R.C.M.P. suggested to the Department of Justice that it was preferable that even in criminal investigations the legislation should provide for authorizations by the Solicitor General of Canada or by provincial attorneys general rather than by judges. The reason given by the R.C.M.P. was that a judge might refuse to grant an authorization to plant a listening device if he were aware that "unorthodox investigative methods" must be employed. It was also suggested that the legislation should contain a specific power to install the device, including the power to make surreptitious entries. This, it was suggested, would be in keeping with the recommendations of the Report of the Canadian Committee on Corrections, 1969, which said that ". . . police powers should be clearly defined and readily accessible". The R.C.M.P. considered that such an express statutory power of entry was necessary despite the existence of subsection 26(2) of the Interpretation Act.[14] Some doubt was expressed as to whether this subsection could be relied upon in these circumstances.

42. Following this, memos were exchanged among various R.C.M.P. and government officials as a result of a suggestion that had been made to the effect that specific provisions authorizing entry were necessary in the proposed legislation dealing with telephone interception both in the Official Secrets Act and the Criminal Code. On April 19, 1972, Mr. Starnes, Director General of the Security Service of the R.C.M.P., in a letter to Mr. Goyer, agreed that the legislation should provide specific provisions for entry upon "telephone company premises, installations, and dwellings generally". Mr. Starnes felt that these provisions should also exempt telephone company employees from liability when acting in good faith and under the direction of a peace officer. Mr. Goyer in turn wrote the Honourable O.E. Lang, then Minister of Justice, to the same effect. Mr. Lang, in reply, assured Mr. Goyer that a peace officer performing his duty under the proposed legislation would have authority to enter premises. He felt that the presence of section 26(2) of the Interpretation

[14] R.S.C. 1970, ch.I-23.

Act was sufficient to cover this matter and therefore there was no need to be specific on this point in the proposed legislation. Consequently no such express power to install, or to enter premises to install (or to enter premises to conduct a survey before the application, or to repair or maintain the device, or to remove it) was included in the legislation, either in respect of interceptions made pursuant to judicial authorizations or those made pursuant to a Solicitor General's warrant.

43. In order to understand this decision it is necessary to cite the relevant provisions of the Interpretation Act and section 25(1) of the Criminal Code:

Interpretation Act:

> 3. (1) Every provision of this Act extends and applies, unless a contrary intention appears, to every enactment, whether enacted before or after the commencement of this Act.
>
> 26. (2) Where power is given to a person, officer or functionary, to do or enforce the doing of any act or thing, all such powers shall be deemed to be also given as are necessary to enable the person, officer or functionary to do or enforce the doing of the act or thing.

Criminal Code:

> 25. (1) Everyone who... is authorized by law to do anything in the administration and enforcement of the law
>
> (b) as a peace officer... is, if he acts on reasonable and probable grounds, justified in doing what he is required or authorized to do and in using as much force as is necessary for that purpose.

44. According to the testimony of Assistant Commissioner T.S. Venner, an oral opinion was given by the Department of Justice to the R.C.M.P. in May 1974, the purport of which was shared by the Legal Branch of the R.C.M.P. This opinion, given before the Protection of Privacy Act came into effect in July 1974, was to the effect that authorizations under the new legislation did not expressly allow for entry into premises, and that the Force would have to rely on section 26(2) of the Interpretation Act and section 25(1) of the Criminal Code to justify such operations. A Legal Branch memorandum dated April 29, 1974, reported on a meeting with Mr. Scollin and Mr. D.H. Christie, Associate Deputy Minister of Justice, at which, according to the memorandum, it was agreed that a sound basis in law for the use of surreptitious entries under the new provisions of the Official Secrets Act was to be found in section 26 of the Interpretation Act.

45. On July 8, 1977, Mr. Louis-Philippe Landry, who was then Assistant Deputy Attorney General, wrote to the Deputy Solicitor General, Mr. Tassé, concerning "allegations of break-ins by members of the R.C.M.P. for the purpose of installing electronic listening devices", which had apparently been discussed recently by them. (Ex. E-1, Tab 2G.) With regard to entries made since July 1, 1974, when an authorization has been issued by a judge pursuant to section 178.13, he wrote:

> When a judge authorizes a peace officer to intercept private communications, the peace officer may, in order to achieve that purpose, enter

> premises in order to install the required electronic devices without the knowledge of the occupant or owner of such premises. I understand that most authorizations given provide for the authorization to enter premises for such purposes. However, even in a case where the judge's authorization is not a specific authorization to enter premises for such a purpose, the officer who installs an electronic listening device for the purpose mentioned in the authorization is not breaking any law.

(As will be seen, we have doubt that, where the authorization was for a listening device, most judges would include an express authorization to enter premises for such purposes. However, conclusive research is impossible because of the statutory provisions against disclosure.)

46. On July 21, 1977, the officer in charge of the Legal Branch argued in a memorandum that, even if section 26(2) of the Interpretation Act and section 25(1) of the Criminal Code gave the implied power to enter to make an installation, it is doubtful that they give the implied power to enter to remove it. However, on November 4, 1977, he wrote to Mr. Landry expressing the view that an authorization of interception implicitly allows the police to remove the device, even after the period stated in the authorization has expired. The Director of the Criminal Law Section of the Department of Justice replied on November 9, 1977, agreeing with that conclusion on the ground that "since the Order authorizes the interception of communications during a specific period of time, it is implicit that the device must be allowed to remain until that time expires".

47. On September 22, 1977, Commissioner Simmonds sent messages to the field directing that no surreptitious entry was to take place to install electronic surveillance equipment unless the words "to install, monitor and remove" are in the authorization received under the Protection of Privacy Act (Ex. E-1, Tab 3G).

48. On June 9, 1978, Mr. Landry wrote letters to all the provincial attorneys general. He stated that the right of a peace officer to enter premises to install or remove an electronic device under the authority of an authorization issued by a judge to intercept telephone communications is possible only if any "terms, conditions, and limitations, included in the authorization are strictly observed". Therefore, in the absence of any limitation on entry into private premises the police officer would be entitled "to enter in order to install (or remove) the device by virtue of section 25 of the Criminal Code and/or section 26(2) of the Interpretation Act, and provided such an entry appears necessary to properly implement the terms of the authorization". As to the right of a police officer to remove an object without the owner's consent in order to install the electronic surveillance device, Mr. Landry had some serious reservations and declined to commit himself one way or the other until the question was examined in depth.

49. By February 13, 1979, after receiving opinions from a number of provincial attorneys general, Mr. Landry's views were strengthened. In a memo of that date, Mr. Landry stated that most of the provinces agreed with his conclusion concerning the first issue stated in his letter of June 9, 1978, though

one province (unspecified) did advance the view that the authorization should contain a clause expressly providing for the installation or removal of the device in order that the peace officer executing the authorization would be protected from civil and criminal liability. With respect to the second issue raised in Mr. Landry's letter there was no consensus among the provinces. Some thought that, in the absence of express removal powers in the authorization, if, for example, a police officer removed a vehicle in order to install a listening device, he would be committing the offence of theft under section 283 of the Criminal Code or the offence of taking a motor vehicle without consent under section 295. Two provinces felt that regardless of the absence of express removal powers in the authorization, a peace officer could take whatever steps were reasonably required to execute the authorization, including the temporary removal of a vehicle. After considering all the opinions Mr. Landry himself opted for the approach that, if it was not specifically provided for by the document authorizing the installation of the electronic surveillance device, then no removal of an object should be undertaken.

50. In December 1977, in *R.* v. *Dass*,[15] Mr. Justice Hamilton of the Manitoba Court of Queen's Bench considered the admissibility of evidence of communications intercepted by use of a listening device installed in premises. He held that an authorization to intercept under section 178.13(2) of the Criminal Code, which extended to both telephonic and oral communications and contained the words "install, make use of, monitor and remove" any device required, authorized a trespass necessary to effect the installation of the device. In April 1979, Mr. Justice Huband in the Manitoba Court of Appeal, delivering the judgment of that court in the *Dass* case,[16] held that evidence obtained from a listening device installed after a surreptitious entry but pursuant to an authorizing order issued under section 178.13 was admissible as "lawfully made" under section 178.16 even if it was made after a break-in, trespass or illegal entry into the premises. He observed:

> How that authorization is carried out is not germane to the issue of the admissibility of evidence flowing from the interception. If a trespass has been committed, then those who have committed the trespass will be answerable in some other criminal or civil forum.

However, in remarks not necessary for the decision but evidently carefully considered, he also specifically rejected an argument presented by Crown Counsel that the authority to install carried with it by implication the authority to enter the premises by force, if necessary, to install the device. Mr. Justice Huband said:[17]

> The order granted by Deniset J. and subsequently renewed by others authorizes the interception, and "for such purposes to install, make use of, monitor and remove" the devices. Crown counsel argues that the authority to install carries with it by implication the authority to enter premises by force or by stealth in order to implant the device.

---

[15] [1978] 3 W.W.R. 762, 3 C.R. (3d) 193, 39 C.C.C. (2d) 465.
[16] [1979] 4 W.W.R. 97.
[17] *Ibid.*, at pp. 116-117.

> As previously noted, the reference to the installation of the authorization order is not a fiat by the courts to violate the laws of the land. I see nothing in the Criminal Code which gives a judge the power to authorize or condone illegal entry. Crown counsel points to s.178.23(2)(d), which appears to enable the judge to impose terms and conditions which he considers advisable in the public interest. In my view, that provision was not intended as a mechanism to have the courts authorize illegal acts. The public interest is not served by acts which violate the civil or criminal laws of the land. The terms and conditions could not validly include permission, directly or by implication, to ignore or breach such laws.

51. Coincidentally, in the same month, the Supreme Court of the United States held in *Dalia* v. *United States*[18] that Congress, in legislating for electronic surveillance under a court order authorizing the installation, maintenance and removal of an interception device, without any statutory limitation on the means necessary to accomplish the electronic surveillance, must have intended to authorize the courts to approve means necessary and reasonable in the circumstances.

52. The R.C.M.P. advised us that as a result of the doubt created by the *Dass* case, some attorneys general issued instructions to the police to cease interceptions where entry was required until the doubt could be removed either by another court or by amendment to the law permitting entry. We requested all attorneys general to inform us as to their position in this regard. A review of the replies received by us indicates that what the R.C.M.P. had told us was correct. Those attorneys general who did not believe that the *Dass* case created doubt as to the legality of entry in appropriate cases cited section 25 of the Code, section 26(2) of the Interpretation Act, and the wording of authorizing orders. One indicated a preference for the reasoning in *Dalia*. Several attorneys general pointed out that, in August 1979, a resolution of the Criminal Law Section of the Uniform Law Conference (a national body formed by the federal and provincial governments to study and encourage uniformity of legislation across Canada) had stated that the power of entry was implied in law. However, the Conference had suggested that the law be amended to provide expressly that an authorization to intercept a private communication under Part IV.1 of the Code be deemed to include authorization to enter premises and install, repair, maintain and remove listening devices, subject to any restrictions imposed by the Court under section 178.13(2)(d).

53. If Mr. Landry's opinion is correct, there are unanswered questions. If a policeman acting under a judicial authorization is on premises surreptitiously to install a listening device, and he is discovered in the act by the occupant who has returned unexpectedly, does the policeman have the implied power, by virtue of section 26(2) of the Interpretation Act, to strike the occupant in order to make his escape? If so, what degree of force may he use? May one of the policemen outside, who is keeping watch, stop the occupant before the occupant reaches his residence, and if "necessary" restrain him by force? Assistant Commissioner Venner told us that the implication is that whatever power is

[18] (1979) 441 U.S. 238.

necessary "within reasonable limits" may be used by the police, who must exercise "judgment" and use "reasonable conduct". He would not assert that such steps would be "legal" but he thought that a policeman would have a defence to a charge (Vol. 33, pp. 5462-7). (We do not know what he meant by drawing the distinction.) We note also that the combined operation of section 26(2) of the Interpretation Act and section 25 of the Criminal Code would, in Mr. Venner's opinion, give the police the power to remove an automobile from its owner's possession in order that a listening device may be secreted in it; at least, there would be "a defence against the charge of theft" (Vol. 33, p. 5463).

54. The same issue applies equally to entry for the purpose of surveying, installing, maintaining and repairing and removing when, pursuant to section 16(2) of the Official Secrets Act, a listening device is to be installed in premises under a warrant of the Solicitor General. Because the procedure employed in conducting electronic eavesdropping under section 16 was, until our public hearings, even less known to the public than that under section 178 of the Criminal Code, and, within the R.C.M.P. and government there does not appear to have been any discussion of this issue in terms of warrants under section 16, there has been little or no analysis of the issue in terms of section 16. However, we do not see any difference between the issue as it arises under section 16 and the issue as it arises under section 178.

55. It will be recalled that *obiter dicta* in the Manitoba Court of Appeal in the *Dass* case said that section 178.13 of the Criminal Code does not empower a judge to include in his authorization a term that authorizes entry into premises for the purpose of installing a listening device. The judgment did not refer to section 25(1) of the Criminal Code or section 26(2) of the Interpretation Act. We understand that those sections were not cited in argument because counsel for the prosecution did not consider them to be relevant. However, that was not the view of the senior officials of the federal Department of Justice in 1979. For example, the Associate Deputy Minister of Justice wrote a letter to the Department of the Solicitor General late in 1979, in respect to a Solicitor General's warrant issued under section 16 of the Official Secrets Act. The opinion expressed in the letter relied not so much on section 26(2) of the Interpretation Act as upon the argument that the legislation could, in large measure, be rendered ineffectual if the interceptions of communications were restricted to those that could be made without any resort to surreptitious or covert entry of premises. Consequently, according to that opinion, only express words or absolutely necessary implication could lead to the construction being properly placed on the legislation that there is no implied power of entry.

56. It therefore becomes necessary to consider those statutory provisions. It will become apparent that in our considered opinion there is real doubt that they support the opinions expressed by the Department of Justice. We say so with considerable boldness and some hesitation, an ambivalence caused by the fact that the opinion of the Department of Justice is supported by the views of some provincial attorneys general and of the Criminal Law Section of the Uniform Law Conference. That being so, we shall give our reasons in some detail.

Does section 25(1) of the Criminal Code justify such an implied power of entry?

57. Section 25(1) derives from a large group of sections in the English Draft Code of 1879, concerning which the Commissioners who had been appointed to consider codifying the criminal law stated that these sections

> . . . contain a series of provisions as to the circumstances which justify the application of force to the person of another against his will. . . We believe that in the main these provisions embody the common law, though on some points they lay down a definite rule where the law is at present doubtful, and in others correct what appear to be defects in the existing law.[19]

The original limitation of the above series of sections, defining the circumstances that justify the *application of force to the person of another*, is still evident throughout sections 25 to 33 of the present Code, wherein constant reference is made to "using as much force as is necessary" or "uses no more force than is reasonably necessary". The same theme is evident in section 25(3) which defines the circumstances in which the use of force that is intended to cause death or grievous bodily harm is justifiable, and in section 25(4) in which the acceptable limits to the use of violence against a person who takes flight to avoid arrest are set forth. It is, therefore, not in our view permissible to suggest that section 25(1) contains a blanket dispensation to peace officers to act in a manner proscribed under the Criminal Code or the common law (e.g. of trespass) in the course of effecting an arrest, or executing a court order or judicial authorization. Moreover, the opinions of the Department of Justice made no reference to the view expressed in the Supreme Court of Canada in *Eccles* v. *Bourque*.[20] The significant issue in that case, for our present purposes, was whether a peace officer who is authorized under section 450(1)(a) of the Code to make an arrest without warrant is also authorized by section 25 to commit a trespass, with or without force, in the accomplishment of that arrest. Five members of the Court were content to reserve their answer to this question until a later occasion. Mr. Justice Dickson, however, in an opinion that was concurred in by three other judges, said:[21]

> It is the submission of counsel for the respondents that a person who is by s.450 authorized to make an arrest is, by s.25, authorized by law to commit a trespass with or without force in the accomplishment of that arrest, provided he acts on reasonable and probable grounds. I cannot agree with this submission. Section 25 does not have such amplitude. The section merely affords justification to a person for doing what he is required or authorized by law to do in the administration or enforcement of the law, if he acts on reasonable and probable grounds, and for using necessary force for the purpose. The question which must be answered in this case, then, is whether the respondents were required or authorized by law to commit a trespass; and not, as their counsel contends, whether they were required or authorized to make an arrest. If they were authorized by law to commit a trespass, the authority for it must be found in the common law for there is nothing in the Criminal Code.

[19] Cmnd. 2345, p. 18.

[20] (1974) 19 C.C.C. (2d) 129.

[21] At p. 130-31.

The same line of reasoning was apparent in the judgment of Mr. Justice Robertson in the earlier disposition of the same case by the British Columbia Court of Appeal:[22]

> . . . it cannot fairly be said that a person who is authorized to make an arrest is, because of s.25, authorized by law to commit a trespass with or without the use of force. In other words, wherever the Criminal Code confers a power to do a specific thing, s.25 does not confer a power to do any and every thing that may assist or advance the exercise of the power. The purpose of s.25(1) is twofold; it absolves of blame anyone who does something that he is required or authorized by law to do, and it empowers such person to use as much force as is necessary for the purpose of doing it.

Another member of the court, Mr. Justice Nemetz did not express any opinion on the scope of section 25(1) other than to observe:

> . . . it is clear to me that, although police officers may arrest without warrant (s.450), scrupulous adherence must be had for the principles set out at common law respecting the procedures that are to be used by police in entering a house without warrant. I do not read s.25(1) as giving a police officer the right forcibly to enter a stranger's home when he is seeking the arrest of a fugitive unless he can justify such forcible entrance on reasonable and probable grounds.

In our view, the opinions of the Department of Justice have failed to take into account the limits of the extent to which section 25(1) affords the power to commit what would ordinarily be trespass or theft. In our opinion, if Mr. Justice Dickson's judgment in *Eccles* v. *Bourque* is (as we think) correct, it requires one to look not to section 25(1) but to the common law for justification for the police power that is asserted. In that case, he found that the common law did empower entry upon premises in order to effect an arrest. In the case of the investigative technique which we are examining, there is no common law precedent of which we are aware which may be called in aid of the power of a peace officer to commit theft or trespass when authorized to install a listening device.

Does section 26(2) of the Interpretation Act justify an implied power of entry?

58. Section 26(2) of the Interpretation Act has already been quoted. Does it apply to an authorization by a judge given under section 178.13 of the Criminal Code or to a warrant issued by the Solicitor General under section 16(2) of the Official Secrets Act? The Act applies to 'enactments', not to judicial orders made pursuant to an enactment. Thus, it could be argued that the power to trespass in order to install a device is implied in section 178; if that is so, there would be an implied statutory power that would permit a judge to include the power of entry in the authorization. However, in the absence of any such term in the authorization, the issue would still remain: is there an implied power of entry once an authorization is granted?

59. In our view, it is doubtful that these provisions provide a defence in law for what otherwise would be theft or trespass. Those who argue that the

[22] (1974) 14 C.C.C. (2d) 279.

Manitoba Court of Appeal in *Dass* was wrong point to the decision of the Supreme Court of the United States in *Dalia* v. *United States*. There, the majority opinion was that the power of surreptitious entry was necessarily implied in the statute that authorized the courts to review and approve electronic surveillance applications. However, in assessing the reasoning of the majority opinion in *Dalia* v. *United States* it is important to note that it emphasized the legislative history of the statute; there was evidence from the Congressional Record that Congress was aware that "most bugging requires covert entry". The opinion also stressed the importance of the fact that "Absent covert entry... almost all electronic bugging would be impossible". In Canada, it is far from clear that either of these points was known to Parliament when the Protection of Privacy Act was passed. Moreover, frequently the entry needed may not be "covert" at all from the point of view of the person who is the owner or occupier at the time of entry — as, for example, a hotel manager who gives permission for the entry before the hotel room is occupied by the suspect, or even while it is occupied by a short-term guest. In such cases there would be no trespass. Many buggings arise in just such situations. Therefore it is not clear to us that Parliament must have realized it was implicitly authorizing trespassory covert entries.

60. However, there is a recent judgment of the British Columbia Court of Appeal in another case, which upheld the implied power of a peace officer to enter a residence to execute a warrant issued under the section of the Code that permits the seizure of firearms.[23] The court held, quite briefly, that in order to give effect to the intent of the section, "we should hold" that the authority to seize "includes the right to search... and includes the right to enter on a person's property to make the search". This decision is a sufficient reminder that a court other than the Manitoba Court of Appeal might reach a conclusion that trespassory entry for the purpose of installation is necessary in order to give effect to a "paramount" public interest to which "the rights of the individual are secondary".[24] Yet, in our view, it is not easy to reconcile the approach of the British Columbia Court of Appeal with that of Mr. Justice Dickson in *Eccles* v. *Bourque*.*

61. In Part X, Chapter 1 we discuss the recent decision of the highest court of England, the House of Lords, in *Morris* v. *Beardmore*. There it was held that a statute that empowered a uniformed police officer to require a person to give a breath sample could not by implication permit an officer to trespass in the suspect's home in order to make the demand. Consequently, if a demand were made during the course of such trespass, the demand would be unlawful and there could not be a conviction for refusal to comply. Lord Diplock said that, "if Parliament intends to authorize the doing of an act which would constitute a tort actionable at the suit of the person to whom the act is done", there must be an express provision to that effect in the statute. He stated that

---

[23] *R.* v. *Colet* [1979] 2 W.W.R. 267.

[24] Using the language of Craig, J.A. who delivered the judgment of the British Columbia Court of Appeal, in respect of the section he was interpreting.

> The presumption is that in the absence of express provision to the contrary Parliament did not intend to authorize tortious conduct.[25]

Applying that reasoning to the *Dass* situation, we believe that it cannot be inferred that Parliament, in enacting a general provision such as is found in section 26(2) of the Interpretation Act, intended that otherwise unlawful powers are deemed to be given to the officer to enable him to do the act which he is empowered to do.

62. We have already mentioned that in August 1979, the Criminal Law Section of the Uniform Law Conference adopted a resolution. Its full terms are as follows:

> WHEREAS the Commissioners are of the view that section 25 of the Criminal Code and section 26 of the Interpretation Act constitute sufficient authority to make it clear for the purposes of Part IV.1 of the Code that lawful authority to intercept includes authority to enter premises and install, repair, maintain and remove listening devices; and
>
> WHEREAS the Commissioners also recognize that the *Dass* case has created sufficient doubt in this area to place the police in a position of uncertainty;
> Be it resolved
>
> that Part IV.1 of the Criminal Code be amended to provide that an authorization to intercept a private communication is deemed to include authorization to enter premises and install, repair, maintain and remove listening devices, subject to any restriction imposed by the Court under s.178.13(2)(d).

[25] [1980] 3 Weekly L.R. 283 at 289.

* On January 27, 1981, four days after this Report was delivered to the Governor in Council, the Supreme Court of Canada delivered judgment in the *Colet* case. In a unanimous judgment delivered by Mr. Justice Ritchie, the judgment of the British Columbia Court of Appeal was reversed and the reasoning of the trial judge was adopted. The trial judge had pointed out that when, in the Criminal Code, Parliament sought to include the right to search in providing for the authority to seize, it did so in specific terms. The court quoted with approval from the judgment of Mr. Justice Dickson in *Eccles* v. *Bourque* and repeated the "common law principle" which "has been firmly engrafted in our law since *Semayne's* case", that "the house of every one is to him as his castle and fortress, as well for his defence against injury and violence, as for his repose...". Mr. Justice Ritchie rejected the argument of the Court of Appeal and said:

> . . . it would in my view be dangerous indeed to hold that the private rights of the individual to the exclusive enjoyment of his own property are to be subject to invasion by police officers whenever they can be said to be acting in the furtherance of the enforcement of any section of the Criminal Code although they are not armed with express authority to justify their action.

Finally, Mr. Justice Ritchie held that section 26(2) of the Interpretation Act could ". . . not be considered as clothing police officers by implication with authority to search when s.105(1) and the warrant issued pursuant thereto are limited to seizure".

The Commissioners did not comment on whether they considered that a present "lawful authority to intercept" includes authority to remove a vehicle from the owner's control, or to use the target's power supply to operate the device, or to use force to restrain a person who appears on the scene.

63. The recommendation of the Uniform Law Commissioners would satisfy the following observation by the Ontario Royal Commission of Inquiry into Civil Rights, chaired by Chief Justice J.C. McRuer:[26]

> When legislation is drawn which is intended to give the power of entry to premises, the power should be stated in clear terms so that when it comes before the members of the Legislature they will know what they are voting on. They ought not to be left to examine the Interpretation Act, or the law applicable to implied powers, when they are required to vote for or against legislation purporting to authorize rights of entry to private property.

If the amendment recommended by the Uniform Law Commissioners is adopted by Parliament, the amendment should be as clear as possible as to whether the police or the security intelligence agency, in exercising the authority granted by the means provided by statute, have all the specific powers that may be required in order successfully to conduct an electronic surveillance operation from beginning to end. The kinds of powers that legislative attention must be addressed to are found in our recommendations in Part V, Chapter 4 and Part X, Chapter 5. If the word "premises" is to include a vehicle or other things, the amendment should be clear whether there is to be a power to remove a thing temporarily without the consent of the person entitled to possession.

64. The power to enter must be strictly circumscribed to prevent any possibility of persons acting under the warrant, in the event of being surprised in the procedure of installation, maintenance, repair or removal, using any physical force against any other person. In the absence of strict statutory prohibition of the use of such force, there is a serious risk that the policeman acting under the authority of a judicial authorization or members of the security intelligence agency acting under a Solicitor General's warrant might consider themselves authorized to use force to restrain a person surprising them during the course of the operation. The danger of this occurring is supported by the opinion given by the Deputy Minister of Justice on February 10, 1978, which stated:

> Subsection 25(1) of the Criminal Code provides, in part, that everyone who is required or authorized by law to do anything in the administration or enforcement of the law as a peace officer is, if he acts on reasonable and probable grounds, justified in doing what he is required or authorized to do and in using as much force as is necessary for that purpose. By virtue of subsection 25(3) a person is not justified in using force that is intended or is likely to cause death or grievous bodily harm, unless he believes on reasonable and probable grounds that it is necessary for the purpose of preserving himself or anything under his protection from death or grievous bodily harm.

---

[26] *Report of the Ontario Royal Commission of Inquiry into Civil Rights*, Toronto, 1968, Vol. 1 at p. 411.

65. For the sake of discussion, let us assume that the intention of Parliament was to enable police officers, armed with a judge's authorization under section 178 of the Criminal Code or a Solicitor General's warrant under section 16 of the Official Secrets Act, to enter premises, remove vehicles, use the target's electrical power supply or restrain persons interfering. If sections 25(1) of the Criminal Code and 26(2) of the Interpretation Act do not entitle a judge or Solicitor General to include express terms to that effect in the authorization or warrant, and if those statutory provisions do not imply such powers where the authorization or warrant is silent, then Parliament's intention is frustrated. However, this would not be the first time that the intention of Parliament has been frustrated by the failure to use language sufficiently clear to give effect to its intention. The remedy is to enact more explicit statutory provisions. It is unsatisfactory to leave these issues unresolved, for otherwise the police and the security intelligence agency will be left uncertain as to the extent to which they are protected by such provisions as section 26(2) of the Interpretation Act and section 25 of the Criminal Code.

66. In Canada the existence of an implied power to enter and do the other things necessary for a successful electronic surveillance, once an authorization or warrant is issued, is uncertain, and so is the power of a judge or the Solicitor General to insert a term in the authorization permitting such entry. In the United States, despite the affirmation by the Supreme Court of the implied power of entry, the government has introduced a bill before the Congress which *expressly* provides for entry and for procedural safeguards to ensure that such methods will be used only when, as the Assistant Attorney General, Criminal Division, has said, "such methods have been found reasonable and necessary by an informed, impartial judicial officer". He continued:

> Briefly, these amendments would require (1) that the application for an order authorizing the interception of communications state whether surreptitious entry will be required to effect the interception and, if so, why other means of effecting the interception are not believed to be feasible, (2) that the issuing judge make a finding that such entry appears necessary under the circumstances, and (3) that the order approving the interception specifically state whether surreptitious entry for the purpose of effecting the interception is authorized.[27]

Therefore we shall recommend in Part V, Chapter 4 that the statutory provision replacing section 16 of the Official Secrets Act specify the incidental powers that are available to those acting pursuant to a warrant; and in Part X, Chapter 5 we shall recommend that section 178 of the Criminal Code be amended by specifying the incidental powers that are available to those acting pursuant to a judicial authorization.

"Rummaging"

67. Another issue common to both the Security Service and the C.I.B. is whether policemen inside premises to install a listening device, having obtained

[27] Statement of Philip B. Heyman before the Committee on the Judiciary, Subcommittee on Criminal Justice, United States Senate, concerning s.1717, March 5, 1980.

either a judicial authorization under section 178 of the Criminal Code or a Solicitor General's warrant under section 16 of the Official Secrets Act, are at liberty to look around, to search for things or documents of possible interest, and to examine and read and photograph what they find of interest? In other words, may they lawfully conduct an intelligence probe? If they may, must it be limited to observing and photographing what is visible to the naked eye without "rummaging", or is the power unlimited? As has been seen in Chapter 2 of this Part, there are judicial decisions which allow the police latitude, when executing a search warrant, lawfully to seize things found by them on the premises even though those things are not referred to in the search warrant. Does the same latitude apply to authorizations and warrants that are *not* warrants to search and seize? In principle there is no practical way of preventing policemen from observing what is readily visible on the premises where the installation is being made, and merely seeing (even with a photographic eye) is no trespass. However, the moment the policeman begins to look through documents, even though their top page is visible, or to open drawers or luggage, there is conduct that is far beyond the necessary activity associated with the installation of a listening device and there may be a trespass. As far as judicial decisions are concerned, there does not appear to be any authority on the point. In Chapter 2 of this part of our Report we saw that there are cases which have held that, within certain limits, a policeman does not become liable for damages for trespass if he exceeds his authority under the search warrant. *Chic Fashions (West Wales), Ltd.* v. *Jones*,[28] which was concerned with search warrants for stolen goods, held that a peace officer may seize under warrant goods not specified in the warrant when he reasonably believes them to have been stolen and to be material evidence on a charge of stealing or receiving against the person in possession of them or anyone associated with him. *Ghani* v. *Jones*[29] suggests that a peace officer may seize from premises which he has entered under warrant, any material of evidential value in connection with the crime he is investigating, whether against the person he is investigating or anyone associated with him in the offence. These English decisions, if they are applied by Canadian courts, go far in permitting policemen to search and seize beyond the terms of a search warrant. Yet they, and earlier authority to the same effect,[30] do not appear to us to support the power of peace officers, armed with an 'authorization' or a 'warrant' to *intercept communications*, to conduct a *search for things*. While the cases cited may be correct in allowing search and seizure of things *beyond the authority of a warrant*, we find it difficult to accept as valid the analogy between that situation and a search when an authorization or warrant does not authorize *any* 'search'. Consequently we entertain, at the very least, serious doubt that there is in law any power to search and look at things while on premises pursuant to an authorization given under section 178.13 of the Criminal Code or a warrant issued under section 16(2) of the Official Secrets Act. Any such power should be provided for in the warrant for surreptitious entry which, as we have indicated in Chapter 2 of this Part, should be granted only in security cases.

[28] [1968] 2 Q.B. 299; [1968] 1 All E.R. 229.
[29] [1970] 1 Q.B. 693; [1969] 3 All E.R. 720.
[30] e.g. *Elias* v. *Pasmore* [1934] 2 K.B. 164.

(b) *Legal and policy issues unique to Security Service*

68. We turn now to a consideration of the procedures adopted when warrants have been applied for under section 16(2) of the Official Secrets Act, which came into effect on July 1, 1974. It will be recalled that this section was passed as part of the Protection of Privacy Act. That statute made it an offence (under Part IV.1 of the Criminal Code and particularly section 178.11(1)) to intercept a private communication wilfully by means of an electromagnetic, acoustic, mechanical or other device, unless the person intercepting has the consent of one of the parties or a judicial authorization. (There are additional protections — for example, for telephone company employees engaged in checking the equipment.) A further defence is provided by section 16(1) for a person who makes an interception pursuant to a warrant issued by the Solicitor General under section 16(2). At this point it is desirable to set forth all the amendments to the Official Secrets Act contained in the Protection of Privacy Act:

> 5. Subsection 2(1) of the Official Secrets Act is amended by adding thereto, immediately after the definition "document", the following definition:
>
> "intercept" includes listen to, record or acquire a communication or acquire the substance, meaning or purport thereof.
>
> 6. The said Act is further amended by adding thereto the following section:
>
> 16. (1) Part IV.1 of the Criminal Code does not apply to any person who makes an interception pursuant to a warrant or to any person who in good faith aids in any way a person whom he has reasonable and probable grounds to believe is acting in accordance with a warrant, and does not affect the admissibility of any evidence obtained thereby and no action lies under Part I.1 of the Crown Liability Act in respect of such an interception.
>
> (2) The Solicitor General of Canada may issue a warrant authorizing the interception or seizure of any communication if he is satisfied by evidence on oath that such interception or seizure is necessary for the prevention or detection of subversive activity directed against Canada or detrimental to the security of Canada or is necessary for the purpose of gathering foreign intelligence information essential to the security of Canada.
>
> (3) For the purposes of subsection (2), "subversive activity" means
>
> (a) espionage or sabotage;
>
> (b) foreign intelligence activities directed toward gathering intelligence information relating to Canada;
>
> (c) activities directed toward accomplishing governmental change within Canada or elsewhere by force or violence or any criminal means;
>
> (d) activities by a foreign power directed toward actual or potential attack or other hostile acts against Canada; or
>
> (e) activities of a foreign terrorist group directed toward the commission of terrorist acts in or against Canada.
>
> (4) A warrant issued pursuant to subsection (2) shall specify
>
> (a) the type of communication to be intercepted or seized;
>
> (b) the person or persons who may make the interception or seizure; and
>
> (c) the length of time for which the warrant is in force.

(5) The Solicitor General of Canada shall, as soon as possible after the end of each year, prepare a report relating to warrants issued pursuant to subsection (2) and to interceptions and seizures made thereunder in the immediately preceding year setting forth

(a) the number of warrants issued pursuant to subsection (2),

(b) the average length of time for which warrants were in force,

(c) a general description of the methods of interception or seizure utilized under the warrants, and

(d) a general assessment of the importance of warrants issued pursuant to subsection (2) for the prevention or detection of subversive activity directed against Canada or detrimental to the security of Canada and for the purpose of gathering foreign intelligence information essential to the security of Canada, and a copy of each such report shall be laid before Parliament forthwith upon completion thereof or, if Parliament is not then sitting, on any of the first fifteen days next thereafter that Parliament is sitting.

Warrants issued before July 1, 1974

69. Before section 16 of the Official Secrets Act came into effect on July 1, 1974, the Security Service wanted to ensure the continuance, without interruption, of telecommunications intercepts and electronic listening devices already installed and in use. Consequently, from June 14, 1974 until the end of that month, the Director General applied for, and the Solicitor General, Mr. Allmand, signed approximately 242 warrants, purporting to be pursuant to section 16 of the Official Secrets Act (Vol. 162, p. 24855). The number 242, which was given *in camera* (Vol. C71, p. 9951), was inadvertently not published in the publicly released version of that evidence. No one — whether Mr. Allmand or Mr. Dare or anyone else — appears to have addressed the question as to whether such warrants had any legal effect on and after July 1. In our view they did not. A statute cannot speak except from the time it comes into effect, and section 16 of the Official Secrets Act did not come into effect until July 1. Only on and after that date could a warrant be issued which would have any status in law. If Parliament intended to give effect to a warrant signed on a date earlier than the date on which the statute came into effect, it would have said so. As a result, in our opinion, although everyone concerned acted in good faith, these warrants were invalid, and in theory those who acted upon them after June 30, 1974 might be open to a charge under section 178 of the Code. We do not think that in the circumstances anyone would think that such charges should be laid. A broader lesson for the future that is afforded by this issue is the need for the security intelligence agency and the Solicitor General having at their disposal informed and competent legal advice, so that issues of this kind may more likely be identified instead of being passed over, unnoticed and unconsidered.

Legal and policy issues relating to the procedure of applying for warrants

70. The following are points arising from the present practice of making applications to the Solicitor General under section 16. A number of the points

give rise to legal concerns, some of which may have escaped the perception of the Director General and his subordinates, and the Solicitor General.

(i) *Renewal procedure*

71. In December of each of the years from 1974 to 1978 the Director General presented to the Solicitor General a document entitled "Application for the Renewal of Warrants to Intercept and/or Seize", which reads as follows:

> This is the application of Michael R. Dare, a member of the Royal Canadian Mounted Police, hereinafter called the applicant, taken before me.
>
> The applicant says he has personally reviewed the applications to obtain warrants to intercept and/or seize, sworn by him during the year 1974, hereinafter called the applications.
>
> The applicant further says in the applications numbered [there followed the number of applications made during the year] his reasonable grounds for suspecting that the communications described therein, or some part of them, are passing, or will pass, still exist.
>
> NOW THEREFORE the applicant prays that the warrants to intercept and/or seize corresponding to the said applications and which would otherwise expire on December 31, 1974, may be renewed.

The Solicitor General then signed a document entitled "Renewal of Warrants to Intercept and/or seize", reading as follows:

> To: The Director General, Security Service, Royal Canadian Mounted Police, and the members and agents of the Royal Canadian Mounted Police acting under his authority or on his behalf.
>
> WHEREAS the Warrants to Intercept and/or Seize under the Official Secrets Act signed by me during the year 1974 are due to expire on December 31, 1974.
>
> AND WHEREAS I am satisfied by evidence on oath of Michael R. DARE, a member of the Royal Canadian Mounted Police, that he has personally reviewed the Applications to obtain the said Warrants sworn by him during the year 1974, and that in the Applications numbered [here the numbers of warrants are inserted] his reasonable grounds for suspecting that the communications described therein, or some part of them, are passing, or will pass, still exist.
>
> NOW THEREFORE you are hereby authorized during the period from the 1st day of January, 1975, to the 31st day of December, 1975, to continue to intercept and/or seize communications under the Warrants signed by me corresponding to the Applications above listed.

As we pointed out earlier there is no provision in section 16 of the Official Secrets Act for renewals of warrants. By way of contrast, section 178.13(3) of the Criminal Code expressly provides that a judge may grant "renewals of an authorization" from time to time. Both sections were enacted in the Protection of Privacy Act. It is a general principle of statutory construction that the statute must be read as a whole, so that if in one circumstance the statute provides for the doing of a thing but in another circumstance the statute does

not provide for the doing of that thing, in the second circumstance it may be inferred that the statute does not authorize the doing of the thing. Applying that principle, in our view there is no statutory authority for the granting of "renewals" of warrants. The result is that a large number of warrants between June and December 1974, all of which were framed so as to expire on December 31, 1974, were not in law effective beyond December 31, 1974. A number of the 1974 warrants were the subject of so-called renewals at the end of 1975, 1976, 1977 and 1978, and were considered by the Security Service to be valid and operative until December 31, 1979. Some of them, of course, were cancelled or allowed to lapse at the end of a calendar year during that period. More warrants were issued in 1975 and were the subject of purported renewal at the end of 1975 and in the succeeding years; and the same was true of new warrants issued in 1976, 1977 and 1978. Thus, during the entire period from January 1, 1975 until December 31, 1978, if we are right in our view of the law, the Solicitor General, lacking the advice of either his Deputy Minister or of the Department of Justice, by signing the so-called "renewal of warrants" each December until 1978, may have inadvertently exposed the members of the R.C.M.P. acting upon the documents to the theoretical possibility of prosecution. However, no doubt, in considering whether those members should be charged under section 178, the Attorney General of Canada or of a province would take into account that the members were relying upon purported renewals of the warrants signed by the Solicitor General of Canada. Moreover, the Attorney General should take into account that on the first occasion when this procedure was used, in December 1974, the renewal forms had been approved by a senior member of the Department of Justice, although it does not appear that any written legal opinion was given by that member of the Department of Justice as to the validity of the procedure which preparation and approval of the forms clearly contemplated would take place each December. In Part V, Chapter 4, we shall make a recommendation as to the procedure which should be provided for by statute when warrants expire.

72. Lest anyone should think that our approach is unduly technical, we hasten to add that there are sound policy grounds for criticizing the procedure adopted in the years 1974 to 1978, in obtaining "renewals". The policy of the statute, as expressed in section 16(2), requires the Solicitor General to be satisfied by evidence on oath "that such interception or seizure is *necessary*" (our emphasis) for one of three purposes. This is a statutory criterion which cannot be satisfied unless there is information placed before the Solicitor General on oath as to why he should find necessity to exist in the circumstances. The so-called applications sworn to by the Director General before the Solicitor General in December of each of the years from 1974 to 1978 did not set forth any grounds upon which the Solicitor General might find that necessity existed. All that the Director General stated on oath was that he had "reasonable grounds for suspecting that the communications described therein, or some part of them, are passing, or will pass, still exist". Thus, even if the applications for "renewal" are looked upon as if they had been styled "applications", and if the "renewal" were treated as if it were a series of "warrants", there was no "evidence" of necessity given on oath, on the basis of which the Solicitor General could grant such "warrants".

(ii) *Swearing of evidence under oath*

73. Section 16(2) authorizes the Solicitor General to issue a warrant "if he is satisfied by evidence on oath". During the early years of the use of section 16, the so-called "application", which was the document purportedly sworn by Mr. Dare, was frequently very brief in terms of describing the activities of the target person or organization, and it stretches the imagination to claim that the bald statement that "such interception or seizure is necessary..." constituted the requisite "evidence on oath" that such interception or seizure was necessary. However, the practice also developed that *aide-mémoires* would be prepared, and that Mr. Dare would bring these with him and show them to the Solicitor General together with the "application". The *aide-mémoire* was not a schedule or annex to the "application", and thus, on the face of the documentation, there was no indication that the truth of the contents of the *aide-mémoire* was sworn to on oath by Mr. Dare. Indeed, Mr. Dare's own evidence was that he did not consider that he was swearing to the truth of the contents of the *aide-mémoire* (Vol. 126, pp. 19647-8). (The accompanying memorandum was, however, being referred to in the form of oath used by Mr. Dare by April 8, 1980, when he last testified on the subject (vol. C88, p. 12186).) Yet Mr. Allmand has testified that he considered that Mr. Dare, in taking the oath before him, was swearing to the truth of all the information which Mr. Dare presented to him (Vol. 115, p. 17756). The Deputy Solicitor General, Mr. Tassé, who was present on many of these occasions, testified that it was customary that Mr. Dare, with Bible in hand, swore "to tell the truth, the whole truth, and nothing but the truth". Although Mr. Tassé understood that Mr. Dare was swearing to the truth of his affirmations or comments, Mr. Tassé did not testify that in the form of oath there was any specific reference to the "evidence" to be found either in the "application" or in the *aide-mémoire* (Vol. 156, p. 23828). Mr. Dare himself testified as to the procedure he was following:

> If it is one or more than one, I stand and take the Bible in my hand and make my attestation. I identify myself as a member of the Royal Canadian Mounted Police, do solemnly swear this or these warrants are required for the security of Canada under the Official Secrets Act. The applicable section of the Act is sworn on each of the warrants.
>
> (Vol. C88, p. 12186.)

He said that "that was the form of oath", although by the time that he testified on April 8, 1980, the word "warrants" is followed by the words "and the accompanying memorandum" (Vol. C88, p. 12186). Thus, if Mr. Dare's evidence is accepted — and it is he who has been personally involved for six years — then it would appear that this practice, as described, has not resulted at all in his swearing to the truth of the statements of fact contained in the application or in the *aide-mémoire*. What he has apparently done is no more than swear to the warrants being "required". (See, in addition to the above testimony, his earlier testimony at Vol. 126, p. 19649.) If his evidence is accepted, then his practice has failed to satisfy the requirement of the statute, for the "evidence" is not "on oath". We do not question the sincerity of Mr. Dare or his subordinates in preparing the material in support of the applica-

tions for warrants or in attempting to comply with the statute. However, the form prescribed by statute was intended to provide some assurance that a Solicitor General would act only on the basis of "evidence" which some person was prepared to verify "on oath". Bearing in mind that the entire procedure by its very nature is very secret, and will never be examined (apart from a Commission of Inquiry such as ours) by any tribunal or by Parliament, it then becomes more than just a matter of form, but rather a matter of form becoming substance, to do the utmost to ensure that the procedure is treated with all the seriousness that is deserved by intrusions into privacy which are numerous and frequently perennial. In Part V, Chapter 4, we shall recommend that the truth of all of the evidence should be sworn to under oath. Here, however, we might add again that the problem we have identified might have been avoided, had legal advice been obtained as to the proper form of the oath to be sworn on these occasions.

(iii) *Identification of the statutory basis in the warrant itself*

74. The warrants issued by the Solicitors General since June 1974 have suffered from what in our opinion is a serious defect. Section 16(2) provides that the Solicitor General may issue a warrant for wiretapping if he is satisfied by evidence on oath that one of the following facts exists:

— that such interception is necessary for the prevention or detection of subversive activity directed against Canada;

— that such interception is necessary for the prevention or detection of subversive activity . . .detrimental to the security of Canada;

— that such interception is necessary for the purpose of gathering foreign intelligence information essential to the security of Canada.

The practice has been that the warrants have simply recited that the Solicitor General is

> satisfied by evidence on oath of Michael R. Dare, a member of the Royal Canadian Mounted Police, that it is necessary for the prevention or detection of subversive activity directed against Canada or detrimental to the security of Canada or is necessary for the purpose of gathering foreign intelligence information essential to the security of Canada to intercept and/or seize any communication hereinafter described. . .

When a search warrant is issued under section 443 of the Criminal Code, it has been held that the offence must be referred to in the warrant.[31] One of the reasons for such a requirement is so that the person whose premises are searched and anyone concerned will know what the alleged offence is, about which evidence is being sought. This reason is inapplicable to warrants issued under section 16(2) of the Official Secrets Act, but another reason may be pertinent: that naming the offence in the search warrant is evidence that the

[31] *R.* v. *Read, ex p. Bird Construction Ltd.* [1966] 2 C.C.C. 137 (Alta S.C.); *Re McAvoy* (1971) 12 C.R.N.S. 56 (N.W.T.S.C.); *Royal American Shows Inc.* v. *The Queen, ex. rel. Hahn* [1975] 6 W.W.R.571 (Alta. S.C.); *PSI Mind Development Institute Ltd.* v. *The Queen* (1977) 37 C.C.C. (2d) 263 (Ont. H.C.J.). There is disagreement in these cases only as to the degree of particularity required to be stated.

justice has exercised his discretion judicially in issuing the search warrant. The same may be said of warrants issued by the Solicitor General under section 16(2): identification of the specific activities being investigated, that is in terms of the three possible alternatives referred to in the subsection, would be evidence that the Minister had exercised his statutory powers with the required degree of attention to the law. Perhaps this would be unimportant if the "evidence on oath" directed the Minister's attention to one of the three heads. However, the so-called "applications" which are the "evidence on oath" have usually *not* indicated which category Mr. Dare has considered the circumstances to fall within. In Part V, Chapter 4 we consider this matter further and make recommendations.

Problems in interpreting the meaning of "subversive activity" (section 16(3))

(i) *"Sabotage"*

75. No warrants have yet been issued under section 16(3)(a) of the Official Secrets Act where the allegation is that the activity in question is "sabotage". However, the Security Service has raised with us a question of definition of "sabotage" as used in this section. The issue is whether the word "sabotage" as used in the section is limited to the traditional dictionary definition of sabotage, i.e. "the malicious waste or destruction of property or manufacturing equipment"? Or, on the other hand, could a warrant be issued where the nature of the sabotage was a systematic sabotage of the "effectiveness or credibility of a federal government institution through the systematic leakage of sensitive or classified documentation entrusted to that person's care"? In the opinion of the Security Service, such systematic leakage "designed to discredit or sabotage the effectiveness of a federal government institution, such as the R.C.M.P. Security Service, could be interpreted as an act to retard an essential public service". The Security Service points to Webster's New International Dictionary, Second Edition, as putting forward a second definition of "sabotage",

> Commission by a civilian or enemy agent within a country of any destructive act designed to impede the Armed Forces, or any act or neglect that retards essential industry, public services, etc.

In our opinion, the word "sabotage" in the absence of any indication to the contrary in the statute, should be interpreted in the normal sense in which it is used as a title to section 52 of the Criminal Code, which makes it an offence to do

> a prohibited act for a purpose prejudicial to
>
> (a) the safety, security or defence of Canada, or
>
> (b) the safety or security of the naval, army or air forces of any state other than Canada that are lawfully present in Canada.

Section 52(2) defines "prohibited act" as meaning

> An act or omission that
>
> (a) impairs the efficiency or impedes the working of any vessel, vehicle, aircraft, machinery, apparatus or other thing, or

(b) causes property, by whomsoever it may be owned, to be lost, damaged or destroyed.

(ii) *"Governmental change"*

76. There is a question as to the meaning of the phrase "activities directed toward accomplishing governmental change within Canada or elsewhere by force or violence or any criminal means" as used in section 16(3)(c). Does it include only activities directed towards the overthrow of a government, or does it cover also activities directed toward accomplishing changes of governmental policies and legislation? The latter appears to be the interpretation of the Security Service, and warrants have been obtained under section 16(3)(c) when the evidence presented to the Solicitor General has in no way suggested that the target person or group had as his or its object anything in the nature of revolution. On the other hand, the former Deputy Solicitor General, Mr. Tassé, has testified that it was his opinion that the narrower interpretation was the correct one, based on the equality of the two official languages for purposes of interpreting a statute, and the fact that the French version of the subsection refers to "changement de gouvernement" (Vol. 157, p. 23884). It is by no means clear that those in the Security Service responsible for the preparation of applications have been aware of that opinion or acted upon it. In Part V, Chapter 4 we shall make recommendations to overcome this ambiguity and narrow the meaning of "subversion".

77. A second question arising in the interpretation of section 16(3)(c), about which the Security Service has expressed concern, is whether it applies to activities by a domestic terrorist group whose activities are politically motivated. We see no problem. As "terrorism" is defined as "violence for political ends", the question itself is redundant. In our view, a domestic terrorist group whose objects fall within section 16(3)(c) in all other respects is one whose activities are covered by the subsection.

78. The Security Service is also concerned as to whether section 16(3)(c) applies to activities directed toward governmental change at provincial and municipal levels. In our view such activities are covered by the section. Some members of the Security Service raise the issue whether the words found in section 16(2) "subversive activity... detrimental to the security of Canada" cover activities that would adversely affect Canadian economic security. The matter has never been put to the test by way of an application to a Solicitor General for a warrant, or even by way of preparing such an application nor does it appear that a legal opinion has ever been sought from the Department of Justice. However, our view is that the intent of section 16(2) is that a warrant may be issued under section 16(2) in respect to "subversive activity" only where there is a form of activity falling within the definition of subversive activity found in section 16(3). Only section 16(3)(b) could apply to the economic field. In our opinion, if the suspected activities were foreign intelligence activities directed toward gathering economic intelligence information relating to Canada, that might not be "detrimental to the security of Canada" in the physical sense, but it would be activity "directed against Canada". Therefore the Solicitor General would be authorized to issue a warrant if he

were satisfied by evidence on oath of the necessity of the interception or seizure of a communication involved in such activity.

(iii) *"Governmental change outside Canada"*

79. An issue of serious concern to the Security Service since January 1978 has been whether section 16(2) authorizes the issue of a warrant where the activity within Canada is directed toward violent governmental change outside Canada. Until January 1978 the Security Service had been under the impression that it could obtain warrants, and it did in fact obtain warrants, where the activities of a person or persons within Canada had been directed toward accomplishing governmental change elsewhere than in Canada by force or violence. Thus, the Security Service had obtained warrants where it could satisfy the Solicitor General that interception or seizure of communications was necessary for the prevention or detection of activity of persons connected with various foreign terrorist organizations. However, in January 1978 the newly arrived Department of Justice counsel gave his opinion that warrants could not be issued in such cases because the governing subsection is subsection (2), which requires that the Solicitor General be satisfied that the interception or seizure of a communication is necessary for one of the following situations:

— the prevention or detection of subversive activity directed against Canada,

— the prevention or detection of subversive activity detrimental to the security of Canada, or

— for the purpose of gathering foreign intelligence information essential to the security of Canada.

Thus, although the activity concerned might fall within the definition found in section 16(3)(c) ("activities directed toward accomplishing governmental change... elsewhere...") it did not fall within any of the above three categories, for, in the opinion of the Department of Justice counsel, such activity was not "directed against Canada" or "detrimental to the security of Canada", or (more obviously) "gathering intelligence information essential to the security of Canada". As a result of his opinion, warrants have not been sought since that time, where the planning takes place in Canada but the target is another country. Examples are the following:

— A landed immigrant was thought to be the leader of a "Liberation Movement" of a foreign country. The field unit represented that there was no way to penetrate the group by human sources, and that therefore electronic eavesdropping was the only way of determining to what degree the organization was involved with a Canadian group considered to be "subversive" or what it was doing that might be detrimental to the security of Canada.

— An application was not processed where the targetted individual was said to be an organizer of a dissident movement in a foreign country where that movement was banned. The Security Service field unit described the movement as pro-Soviet and as advocating the overthrow of its own government.

— A similar example was that of a proposed warrant against communications of a foreign "leftist" thought to belong to a revolutionary movement in his country of origin and to be a leader of his countrymen in a Canadian city.

80. We question the correctness of the legal opinion upon which this reticence by the Security Service has been founded since 1978. We recognize that the matter is not free from doubt, and we certainly do not criticize counsel for the Department of Justice for giving the opinion which he gave. Our view is based on mounting experience around the world, that one of the increasingly common ways in which terrorist groups attack a country is not within its own borders but outside its borders, as for example, by attacks on that country's missions abroad or its mission personnel abroad. Thus, there is a strong possibility that a foreign terrorist group whose members in Canada are suspected of actively planning terrorist acts against their homeland may plan to do so by attacking the mission premises or mission personnel of their homeland located in Canada. Moreover, in our opinion, any such terrorist acts are quite properly described as "activities directed against Canada or detrimental to the security of Canada". It is activity "directed against Canada" in that Canada has a duty under international law, and under domestic statute law, to protect foreign mission property and personnel. A failure to afford reasonable protection is a breach of international and domestic law. Consequently, any conduct directed toward attacking foreign mission premises or personnel is "directed against Canada". It may also be said to be "detrimental to the security of Canada". We think that the legislation should be amended to make it clear that activity of the kind just discussed may be the subject of a warrant authorizing the interception or seizure of communications.

81. It follows from the same opinion by counsel for the Department of Justice that the Solicitor General should not grant a warrant where it is clear that the sole target of foreign terrorists in Canada is against the foreign country on its own territory or at least outside Canada. Again, we think that terrorist activity that is being planned and supported in Canada, regardless of whether it is targetted against Canada or a foreign country, can threaten the security of Canada. The failure to keep such activity under surveillance may disable Canada from discharging its obligations under international agreements to prevent terrorism. The definition of threats to the security of Canada which we shall recommend in Part V as a statutory limit to security intelligence surveillance will cover terrorist activity in Canada against foreign governments.

(iv) *"Foreign"*

82. Doubt exists within the Security Service as to whether the use of the word "foreign" in section 16(3) includes Commonwealth countries. In our opinion, by analogy with Canadian court decisions interpreting other statutes, the word "foreign" does include all other countries, including Commonwealth countries. Should it continue to be felt there is any doubt on this matter the doubt should be resolved by legislation.

83. We have not reviewed all the warrants issued since July 1, 1974, but among those we have considered there are some instances in which it is

difficult to see that the activity of the target person or group was in any way within section 16(2) and (3). Either the police forces or the security intelligence agency (we have doubts as to whether it should be the latter) should be concerned to detect and prevent the activities of such a person and group, in so far as they are directed toward damaging the property of other persons and otherwise violating the Criminal Code and other laws. Yet, we find it difficult to imagine that their activities can properly be described, in any real sense, as "directed toward accomplishing governmental change within Canada".

What does "specify" mean in section 16(4)?

84. A legal question which appears to have gone unnoticed by the Security Service and Solicitors General is that section 16(4)(b) requires the warrant to "specify"

> . . . the person or persons who may make the interception or seizure.

What is the meaning of the word "specify"? No such word is found in section 443, concerning search warrants to be issued by a Justice of the Peace, which provides that the form of warrant shall be directed "to the Peace Officers in the (territorial division)". Section 178.13(2) of the Criminal Code, relating to electronic interceptions of private communications, requires that the authorization "generally describe the manner of interception that may be used" but does not say anything about the person who is to be authorized to make the interception. However, section 178.13(2.1) reads:

> The Solicitor General of Canada or the Attorney General, as the case may be, may delegate a person or persons who may intercept private communications under authorization.

Therefore, neither the provisions for search warrants nor for electronic interception in criminal investigations is of assistance in interpreting section 16(4)(b). The Concise Oxford Dictionary defines the verb "specify" as follows:

> Name expressly, mention definitely.

Webster's New Collegiate Dictionary defines "specify" as follows:

> To name or state explicitly or in detail.

The form of warrant under section 16, prepared by the Department of Justice before July 1, 1974, is directed as follows:

> 2. To the Director General, Security Service, Royal Canadian Mounted Police, and the Members and agents of the Royal Canadian Mounted Police acting under his authority or on his behalf.

We have serious doubts that such a direction complies with the requirement of section 16(4) that the warrant "specify" the person or persons who may make the interception or seizure. Any statutory revision of section 16 should remove this doubt, so as to ensure that the warrants do protect members of the security intelligence agency, and for that matter, that they protect the officials of telephone companies co-operating with the security intelligence agency, who at present may be parties to an interception but cannot be said to be "agents" of the R.C.M.P. acting under the authority of the Director General or on his behalf.

Can a warrant be issued under section 16(2) to intercept or seize written communications?

85. During the first two years of the operation of section 16, the warrants which were issued related to the interception of communications by wiretapping (principally telephonic communications), and by microphone operations (called "oral" communications in the jargon of the Security Service). In 1976, in the investigation of the Omura case, application was made to the Solicitor General for a warrant to authorize the interception of postal communications of a person believed to be associated with Omura. The Solicitor General, Mr. Allmand, signed the warrant but on condition that it not be executed except upon an opinion being received from the Department of Justice that the warrant was valid. On June 14, 1976, the Deputy Minister of Justice, Mr. D.S. Thorson, Q.C., by letter to Mr. Allmand, advised as follows:

> I am of the opinion that the word 'communication' in section 16(2) of the Act includes letters. However, section 43 of the Post Office Act reads as follows:
>
> > 'Notwithstanding anything in any other act or law, nothing is liable to demand, seizure or detention while in the course of post, except as provided in this Act or the regulations. R.S.c.212, s.41.'
>
> In view of the clear wording of the above noted section in the Post Office Act, section 16(2) of the Official Secrets Act cannot, in my opinion, be interpreted as taking precedence over section 43 of the Post Office Act.

For present purposes, the significant portion of Mr. Thorson's letter is his one sentence opinion that the word "communication" in section 16(2) of the Official Secrets Act includes letters. In consequence, one warrant was obtained in May 1976, authorizing the interception of "written communications" of a target organization. Mr. Tassé testified that early in 1977, while he was still Deputy Solicitor General, a further opinion, this time verbal, was obtained from the Department of Justice that section 16 authorized the interception or seizure of "written" communications (Vol. 156, p. 23814). Later in 1977, having become Deputy Minister of Justice, Mr. Tassé signed a written opinion to the same effect. Consequently, since then the Security Service and the successive Solicitors General have considered section 16 to authorize the issuing of warrants to intercept and seize "written communications". In our view, there is a serious question as to whether section 16(2) authorizes the issuing of a warrant to intercept or seize "written communications". The amendment to the Official Secrets Act in 1973 was part of the Protection of Privacy Act, the principal provision of which made it an offence to "wilfully intercept a private communication. . . by means of an electromagnetic, accoustic, mechanical or other device". The provisions of the amendment to the Official Secrets Act must be read in the context of the Protection of Privacy Act as a whole unless there is some indication in the statute that the Official Secrets Act amendment is to be read differently. As was said by Mr. Justice McIntyre in the Supreme Court of Canada:

> It was said that well-established canons of construction dictated that words should receive a uniform meaning when used repeatedly in the same statute or in one *in pari materia*. Following this principle, it was said, the separate

> parts of the Protection of Privacy Act which amended the Criminal Code, the Crown Liability Act and the Official Secrets Act, respectively, should be construed as a unified whole, providing one body of law applying to the separate situations covered by the separate Acts which were amended. I have no quarrel with the general proposition thus expressed...[32]

The amendment to the Official Secrets Act created an exception to the criminal liability imposed by the principal part of the Protection of Privacy Act:

> 16. (1) Part IV.1 of the Criminal Code does not apply to any person who makes an interception pursuant to a warrant. . .

This does not mean that one can read section 16 without regard to the provisions of Part IV.1 of the Criminal Code, for both provisions formed part of the Protection of Privacy Act. Moreover, unless there is language leading to a contrary construction, the language of section 16(1) and (2) must be read as providing a defence to what section 178 of the Criminal Code makes an offence, and sections 16(1) and (2) must not be read as providing a statutory procedure for authorizing something which is otherwise no offence under section 178. Thus "communication" as used in section 16(2), not being defined in the amendment to the Official Secrets Act, must be given the same meaning as in the remainder of the Protection of Privacy Act. In the principal part of the Protection of Privacy Act, which enacted section 178 of the Criminal Code, the word "communication" is defined only as part of the definition of the expression "private communication". Part of the definition of that expression in section 178.1 reads:

> Any oral communication or any telecommunication. . .

(The balance of the definition relates to the word "private", which has no relevance to section 16 of the Official Secrets Act.) There is only one respect in which section 16(2) may contain an indication that it is meant to apply to communications of a broader or different kind than those with which the balance of the Protection of Privacy Act was concerned: the word "seizure" may imply that written communications are included within the purview of section 16(2). However, we doubt that that element overcomes the reasoning previously stated. Thus, in our opinion, it is at least doubtful that section 16(2) of the Official Secrets Act can be read as authorizing the Solicitor General to issue a warrant in respect of written communications of any kind, whether letters in the post or other written communications (other than telegraphs, cables and telexes, which would be "telecommunications"). Therefore, if there is to be legislation permitting the opening of mail for security purposes, section 16 of the Official Secrets Act would have to be amended further than needed merely to provide that its provisions override the provisions of the Post Office Act; section 16 would have to contain language redefining "communication". Moreover, if section 16 is to be taken as authority for the issuing of warrants for the seizure or copying or photographing of some forms of written communication in the course of post, other than letters, (e.g. printed books, typed books, accounting records and code books), which may not properly be described as

[32] *Goldman* v. *Regina* (1980) 51 C.C.C. (2d) 1 at 19; 13 C.R. (3d) 228 at 251.

"communications", the legislation should be amended to empower the Solicitor General to issue a warrant authorizing such acts. It follows from our reasoning that if the Bill introduced in Parliament in January 1978 had been enacted, it would not have achieved its intended purpose.

Use of section 16 warrants for purposes of search

86. After July 1, 1974, the Security Service was concerned as to the means by which it should gain approval for "PUMA" operations, that is, operations involving surreptitious entry upon premises to search and examine articles on the premises and copy or photograph them. In the early period of the operation of section 16, the Security Service considered that the use of warrants issued by the Solicitor General authorizing the interception of oral communications was an umbrella for PUMA operations which was "not entirely appropriate but better than nothing". In two cases the Security Service applied for warrants under section 16 under the representation that the interception or seizure of the targetted individual or group's communications was necessary for the prevention or detection of subversive activity, when the real intention and sole object of the Security Service was not to intercept oral communications but rather to search, examine, copy and photograph articles found on the premises where the electronic device was to be installed. We are not suggesting any impropriety in these two cases; the members involved in preparing the applications thought that they were following the proper procedure for obtaining authority for such a search. Other than these two cases, it can be said that the Security Service considered that where it could find the grounds to support a genuine application under section 16, it was then consciously prepared, when entering the premises to install a listening device, to have its members seize the opportunity to search, examine, copy and photograph. This continues to be the approach of the Security Service. Whether this is a lawful practice has already been discussed under the title "Rummaging", earlier in this chapter.

Use of information obtained through warrants issued under section 16

87. There is a deficiency in section 16 of the Official Secrets Act from the point of view of providing protection for members of the Security Service who communicate the content or purport of a communication intercepted under a section 16 warrant to a friendly foreign agency. For example, one may reasonably expect information obtained by our security intelligence agency about an international terrorist, who is in Canada, to be transmitted to the agency of another country which shares Canadian concerns about the person's future activities. If the Canadian security intelligence agency does not provide information it has of that nature to friendly agencies, they in turn are unlikely to give the Canadian agency information they have that may be of interest to Canada. Reciprocity is expected. If the information has been obtained as a result of electronic interception of communications, there may be a serious legal problem in this action. It arises from section 178.2(1) of the Criminal Code, which prohibits the wilful use or disclosure of a private communication "or any part thereof or the substance, meaning or purport thereof or of any part thereof" without the consent of one of the parties to the communication;

but subsection (2) provides that that does not apply to a person who makes any such disclosure

(a) in the course of or for the purpose of giving evidence in any civil or criminal proceedings or in any other proceedings in which he may be required to give evidence on oath where the private communication is admissible as evidence under section 178.16 or would be admissible under that section if it applied in respect of the proceedings;

(b) in the course of or for the purpose of any criminal investigation if the private communication was lawfully intercepted;

(c) in giving notice under section 178.16 or furnishing further particulars pursuant to an order under section 178.17;

(d) in the course of the operation of

(i) a telephone, telegraph or other communication service to the public, or

(ii) a department or agency of the Government of Canada,

if the disclosure is necessarily incidental to an interception described in paragraph 178.11(2)(c) or (d); or

(e) where disclosure is made to a peace officer and is intended to be in the interests of the administration of justice.

None of these exceptions appears to protect a member of the R.C.M.P. Security Service who discloses such information to the security intelligence agency of another country. We shall recommend that statutory protection be extended to such an employee of the security intelligence agency. (See Part V, Chapter 4.)

88. There is legal protection for the employee of the Security Service who listens to the intercepted communication and translates or transcribes it, because section 16(1) of the Official Secrets Act says that Part IV of the Code does not apply to a person who makes an interception pursuant to a warrant or to any person who aids him. However, what about the employee or member of the Security Service to whom the transcript is delivered, who then analyses it and condenses it into a report which is placed on file for other members to read or which is transmitted to other members or even to other departments of the government? None of the exceptions contained in section 178.2(1) affords protection to him. Nor does section 16(1) of the Official Secrets Act afford protection, for it cannot be said that any of those persons are persons who "in any way" aid the person making the interception. Consequently we shall recommend that protection be afforded to such persons by amendment to section 16, when disclosure is made to any person for the purposes of carrying out the functions of the security intelligence agency and subject to strict guidelines about reporting security intelligence. (See Part V, Chapter 4.)

Miscellaneous legal issues arising from the technical aspects of electronic surveillance

89. There are a number of legal issues that require resolution if the security intelligence organization is to be able to carry out its responsibilities once a warrant is issued authorizing electronic interception of communications.

90. The R.C.M.P. identified as a problem the possibility that radio transmitters installed pursuant to a warrant issued under section 16 of the Official Secrets Act might violate the licensing requirements of the Radio Act. That problem was resolved in 1979 when the Minister responsible under the Radio Act granted a blanket licence for the use of "any and all types of radio apparatus to be used by persons acting under the direction of the Director General of the Security Service in the course of investigations related to national security matters, which radio apparatus is of a special design for which the prescribed procedures for technical approval and acceptance are not appropriate". Such a licence is permissible under section 4(1)(b) of the Radio Act. Thus, while there no longer is a legal problem, we note that until 1979 microphone operations may have violated the provisions of the Radio Act.

91. Another concern is that members of the R.C.M.P. engaged in making the technical installation may be violating the requirements of provincial laws regulating the qualifications of persons making electrical installations. (The problem presumably exists also in the case of installations made in the course of criminal investigations under section 178 of the Criminal Code.) A similar problem arises when the Security Service makes a major electrical installation in its own premises, whether at Headquarters or elsewhere across the country — for example, for the reception of electronically eavesdropped conversations. The Security Service does not have personnel who meet the residency requirements of all the provinces. The use of contracted personnel bears inherent security risks. Apart from accepting such risks and contracting with outside personnel, we can recommend no other course but to negotiate lawful administrative arrangements with the provincial authorities and, if necessary, request exemptive provincial legislation to cover the specific need. We realize that this problem, and the problem discussed in the next two paragraphs, may in law be non-existent if a correct interpretation of the judicial decisions on the Constitution would lead to the conclusion that such works and undertakings by the R.C.M.P. would not be subject to provincial regulatory laws. However, the answer to that question, short of going to court for a ruling, must remain uncertain. Therefore we think it best that it be assumed that provincial law is applicable and that negotiations with the provincial authorities be carried out.

92. Another concern is that the installation of equipment in 'observation posts' and 'listening posts' — houses, apartments and offices from which to observe actions and receive intercepted communications at nearby targetted premises — may violate provincial and municipal laws, such as fire regulations. The Security Service wishes to avoid having to comply with such regulations because compliance, meaning permits and inspections, might endanger the security of such operations. Moreover, the nature of the installation is frequently such that the security intelligence organization will be unable to meet the minimum provincial or municipal standards of protection. We can see no alternative but to ask provincial governments to amend relevant statutes to exempt such installations. In the specific case of fire regulations, for example, the standards of protection should be inspected in all such posts by an inspector of the office of the Dominion Fire Commissioner. There is already an inspector in that office who has the requisite security clearance and inspects restricted areas in buildings owned by the R.C.M.P. Security Service.

93. A similar concern is that provincial and municipal building codes may be violated by structural alterations that may have to be made to premises used as observation posts or listening posts. This may consist of the construction of false walls, modifications to plumbing, etc. Applications for permits and examination by provincial or municipal inspectors would endanger the security of the operation. We doubt that many of the alterations to premises required by such operations would constitute such 'construction' or 'demolition' of a 'building' as would violate the typical provincial statute which prohibits such construction without a permit, or would constitute violation of the typical provincial statute which prohibits a 'material change' in a plan on the basis of which a permit was issued without satisfying the authorities. Nevertheless, because of the possibility that violations might occur, we think that provincial governments should be asked to amend building code legislation to exempt such alterations provided that they do not weaken the structure of, or otherwise endanger, a building, or result in an occupant being subjected to an unreasonable danger.

94. Another concern is that sometimes the method of eavesdropping, when authorized under section 16 of the Official Secrets Act, is by means not of a wire microphone or a battery-operated radio transmitter but by a transmitter which is powered by the power supply paid for by the subject of investigation or another person. This may constitute an offence under section 287 of the Criminal Code, which provides as follows:

> 287. (1) Every one commits theft who fraudulently, maliciously, or without colour of right, (a) abstracts, consumes or uses electricity or gas or causes it to be wasted or diverted. . .

It might be argued that the Solicitor General's warrant gave the accused a "colour of right" — i.e. a belief that he had a right to take "possession" of the electricity for the purposes of the authorized interception — although we do not subscribe to the validity of such an argument. To remove the lingering concern, we shall recommend that the amendments to the legislation expressly empower the use of devices that operate by using the electrical power supply found upon the premises. We are advised that the value of the amount of power thus used is a matter of cents per month, and we do not consider the burden thus placed upon the suspect or neighbour to be significant. (The same solution should apply on the side of criminal investigations, to section 178 of the Criminal Code.)

Importing highly sensitive equipment

95. Occasionally the Security Service, wishes to bring into Canada novel and effective surveillance equipment, designed to detect communications and observe conduct, which it would be too costly to manufacture in Canada. On these occasions, the Security Service is properly concerned to reduce to a minimum the number of people who know of the existence of this means of detection and its capabilities. Therefore the Security Service has wished to avoid inspection of such items by customs officers.

96. The Customs Act contains no provisions exempting any goods imported into Canada from being examined by the Customs and Excise Branch. In fact,

in the case of another federal government department, military equipment is imported without inspection by virtue of an arrangement under which the customs officer is instructed not to inspect the goods. However, we believe that a better and firmer solution should be found. An administrative solution that would be preferable would see one Customs inspector being given the requisite security clearance to attend to all such imports. If that should prove unworkable, we consider that the legislation chartering the security intelligence organization should expressly exempt from the provisions of the Customs Act such equipment as may be required by the organization for its purposes, such requirement to be certified by a certificate of the Director General attached to the particular goods.

Does the Diplomatic and Consular Privileges and Immunities Act raise any impediment to a Canadian security intelligence agency's work in countering espionage?

97. The Vienna Conventions on Diplomatic and Consular Relations were signed by Canada on February 5, 1962, and have been part of Canadian domestic law since June 29, 1977, as a result of the enactment of the Diplomatic and Consular Privileges and Immunities Act. Section 2(1) of the Act states that certain Articles of the Vienna Convention on Diplomatic Relations and of the Vienna Convention on Consular Relations "have the force of law in Canada in respect of all countries (including Commonwealth countries), whether or not a party to the conventions." The provisions of the two Conventions are substantially the same. Reference will be made only to the Convention on Diplomatic Relations. The following are articles from that Convention which, in the schedule to the Act, have the force of law in Canada:[33]

> 22.1. The premises of the mission shall be inviolable. Agents of the receiving State may not enter them, except with the consent of the head of the mission.
>
> 2. The receiving State is under a special duty to take all appropriate steps to protect the premises of the mission against any intrusion or damage and to prevent any disturbance of the peace of the mission or impairment of its dignity.
>
> 27.1. The receiving State shall permit and protect free communication on the part of the mission for all official purposes. In communicating with the Government and the other missions and consulates of the sending State, wherever situated, the mission may employ all appropriate means, including diplomatic couriers and messages in code or cipher. However, the mission may install and use a wireless transmitter only with the consent of the receiving State.
>
> 2. The official correspondence of the mission shall be inviolable. Official correspondence means all correspondence relating to the mission and its functions.

98. The following legal issues have been raised:

(a) Is it Canadian law that a violation of the provisions of Articles 22 and 27 of the convention occurs if the telephone lines of a foreign mission

[33] S.C. 1976-77, ch. 31.

were to be tapped or a listening device were to be installed and used in the premises of a foreign mission?

(b) Is it Canadian law that a violation of the provisions of the convention occurs if the security intelligence agency were to have a human source inside a foreign mission?

(c) Is it Canadian law that a violation of the provisions of the convention occurs if the security intelligence agency were to have a member or other person enter the premises of a foreign mission, under a pretext?

99. Some introductory remarks are in order, concerning customary international law, the Conventions and the statute. In customary international law, the inviolability of diplomatic premises has long been recognized as subject to the overriding principle that the embassy must not be used to the detriment of the host country or for the purpose of infringing the law of that country. The best known example of not accepting the inviolability as absolute arose in 1896, when the British Government announced its intention to invade the Chinese embassy in London in order to rescue Sun Yat-Sen, who was being held in the embassy against his will with the object of sending him back to China. The purpose of a mission is to represent the views of its country to the host state. The mission is not entitled to engage in espionage or endanger the security of the host state. Nor is the host state required to tolerate activities by the mission which go beyond its proper function. The host state is entitled to take such measures as are necessary to preserve its own security. If the mission abuses its rights, the host state is entitled to take measures to counter such activities, so long as they remain proportionate in character. The foregoing principles however, do not provide guidance on the key question of the rights of the host state when it comes to the acquiring of information concerning the possibility of violations of diplomatic privileges and immunities. We are, however, persuaded that the host state has a right to acquire knowledge of whether the persons who enjoy the privileges and immunities recognized by the Convention are violating their own duty not to interfere in the affairs of the host state. It therefore follows that the host state has the right to take reasonable steps to acquire such knowledge.

100. While normally a treaty would be regarded as overriding the principles of customary law, this is true only when the treaty is a law-making document. In the case of the Convention, the purpose was to codify what were regarded as being the customary and accepted rules on the subject, and to provide some text which would be acceptable to the new states, many of which have contended that there is no true customary law in existence, since what is described as being such law came into being before the creation of those states and without their consent. To this extent, therefore, in so far as the text of the Convention does not expressly overrule accepted rules of customary law, these are considered to be still in existence. The Convention is confirmatory of international customary law and to the extent that it does not expressly override such law it leaves it intact (see, for example, *The Amazone*[34]).

[34] [1940] P. 40. This case referred to the Diplomatic Privileges Act, 1708, as being declaratory and not exhaustive of diplomatic privileges, so that in so far as the Act was silent the privileges of customary law still existed.

Secondly, when codificatory instruments are being drafted it is not the practice to list all the exceptions and waiver possibilities, particularly when state practice over the centuries has recognized the possibility of even the invasion of an embassy.

101. It cannot be presumed that Parliament intended to legislate in a way that would inhibit protective action, especially as such action is compatible with the principles of customary international law concerning diplomatic privileges and immunities. The statute is principally concerned with acts taken by private individuals, which may contravene the rights of diplomatic missions, and not acts by state agents or on behalf of the state. It does nothing more than to give modern legislative form to what has been the position under customary law, both national and international, with regard to the protection of diplomats. The obligation upon the receiving state to protect the mission from intrusion and the like relates to the activities of private interests and does not create any criminal liability in respect of acts interfering with the mission's security undertaken by or on behalf of the host state.

102. The purposes of the inviolability provisions of Article 22 are to enable the mission to function peacefully and without interference, to prevent the host state from inhibiting such activities by unwarranted interference, and to secure the mission from illegal activities by local residents. The aim is to enable the mission to carry out its proper activities (which are set forth in Article 3 of the Convention).

103. Article 22 does not protect the mission in so far as the mission goes beyond the purposes for which it had been accepted. Article 41.1 forbids interference in the internal affairs of the host state, and Article 41.3 forbids use of the premises of the mission "in any manner incompatible with the functions of the mission as laid down in the present convention or by other rules of general international law or by any special agreements in force between the sending and the receiving State." Thus, if an embassy were being used as a "prison" for nationals of either the host or the sending country, the mission would be violating the provisions of Article 41.1 and 41.3, and Article 22, the purpose of which is to enable the mission to perform its proper functions peacefully and without interference. The purpose of those articles is not to preclude the local authorities from entering the embassy.

104. As far as telephonic communications to and from the mission are concerned, if they concern activities which are beyond the proper activities of the mission, by the same reasoning Article 27 would not be violated by the host state taking steps to detect such communications. In any event, provided that the steps taken to "wiretap" occur outside the mission premises, there is no question of a violation of such premises. Moreover, as far as Article 27 is concerned, such listening does not obstruct or inhibit "free communication on the part of the mission for all official purposes".

105. If the electronic surveillance is by a microphone installed in the premises, where the host state has grounds for suspecting activities on the part of the mission beyond the appropriate functions of the mission, in our view there is no violation of either Article 22 or Article 27.

106. Nor, in our view, does Article 22 prevent the security intelligence agency of the host state from having a human source inside the mission, or from having a person enter the mission premises under a pretext. When Article 22 refers to entry, there is little doubt that the draftsmen had in mind a physical invasion. They were concerned with enabling the officers of the mission to fulfill their tasks without threats or fears of bodily harm by local nationals invading the premises. Article 22 does not preclude the host state taking measures of anticipatory self-defence, for example by obtaining information as to whether there has been an abuse of the mission's functions.

107. Our conclusion is that the use of certain investigative techniques, when there are grounds to suspect that the mission's staff is engaged in espionage, would not result in an offence being committed under section 115 of the Criminal Code, for there is a "lawful excuse" for such conduct. Moreover, persons involved in such conduct in the course of the investigation of suspected espionage could not be said to be "wilfully" omitting to do anything which is required to be done by any of the articles of the Diplomatic and Consular Privileges and Immunities Act.

(c) *Legal and policy issues unique to the C.I.B.*

108. The 1979 Annual Report prepared by the Solicitor General of Canada and laid before Parliament in 1980, pursuant to section 178.22 of the Criminal Code noted somewhat obscurely that the following was an area of concern:

> The provisions regarding the disclosure of information by electronic surveillance. These provisions impede rather than facilitate international exchanges of information.

This no doubt is a reference to a problem that the R.C.M.P. has drawn to our attention as to whether members of the R.C.M.P. may give to a foreign law enforcement agency any information which the R.C.M.P. obtains from electronic surveillance. In the discussion of legal and policy issues concerning the Security Service we have mentioned the offence created by section 178.2(1) of the Criminal Code for disclosure of the content or purport of a communication, and the exceptions provided by subsection (2). None of these exceptions appears to protect a member of the R.C.M.P. who discloses such information to a foreign agency, unless it can be said that (e) is applicable, which is doubtful. We shall recommend that section 178.2(1) be amended to make it clear that such information may lawfully be given to a foreign law enforcement agency.

109. Another aspect of the limited exceptions is that members of the R.C.M.P. are severely restricted as to what information they may give to anyone involved in the preparation of the Annual Reports of the Solicitor General of Canada and the provincial attorneys general. Consequently the Annual Reports are likely to be less informative than they should be as to the value of the intelligence product received, unless evidence adduced in court has resulted. This limitation equally would severely impede any attempt in the future, whether within the R.C.M.P. or by any other body, to conduct an assessment of the benefits of electronic surveillance in comparison with the tangible and intangible costs of such operations. We shall recommend that

section 178.2(1) be amended to make it clear that such information may lawfully be given to any person, whether that person is a peace officer or not, who is involved in the preparation of the Annual Reports.

110. Our examination of the operation of section 178 of the Criminal Code has been limited to consideration of the procedure by which applications are made to a judge for an authorization. We did not think that consideration of the entirety of section 178 was within our terms of reference. For there have been no suggestions made to us that in some respect the R.C.M.P. has been using section 178 in a way that is "not authorized or provided for by law"; consequently consideration of section 178 as a whole would not fall within paragraph (a) of our terms of reference. Nor does it fall within paragraph (c), for section 178 has not in practice been used as a means of obtaining authority for the Security Service to conduct electronic interception of communications. However, we did address our attention to the application procedure because we wanted to have a good grasp of how it is functioning, in case some aspect of the procedure would have a bearing on the procedure that might be used if the law is amended to permit the opening of mail for purposes of any criminal investigations, a subject that was certainly within the terms of reference because of past practices "not authorized or provided for by law". Whatever our recommendation might be in that regard, we knew that the Bill introduced in Parliament in January 1978 proposed that the procedure by which an application for judicial authorization would be made should be akin to that already provided for in the case of electronic interception. Therefore it seemed to us that it was important to examine the existing application procedures.

111. However, this was not an easy task. Section 178.14 of the Criminal Code requires all documents relating to an application to be treated as confidential. Further, all the documents except the authorization itself are required to be placed in a packet and sealed by the judge. The packet is to be kept in the custody of the court and is not to be opened except for the purpose of dealing with an application for renewal of the authorization, or pursuant to an order of a judge. An application was made on behalf of a provincial judicial inquiry for an order to open a packet so that the inquiry might examine the affidavit, but the Chief Justice of the Trial Division of the Supreme Court of Alberta refused to make the order sought.[35] Thus it is apparent that at present the Code does not permit a Commission of Inquiry to gain access to affidavits sealed in packets, to examine the quality of the documentation filed in support of authorizations that have been given. Moreover, to comply with the spirit of section 178.14, the Department of Justice and the R.C.M.P. do not retain copies of the applications once the authorization has been granted. So, even if the Department were prepared to give us access to such documents, they are simply not available for inspection. While on the one hand the law and the administrative practice thus genuinely further the statutory objective of confidentiality, on the other hand they render it impossible to assess the quality of the documentation other than by questioning some of those who since 1974 have been involved in the application process. This we have done, and while so

[35] *Re Royal Commission Inquiry into the Activities of Royal American Shows Inc. (No. 3)*, (1978) 40 C.C.C. (2d) 212.

doing we have explored with them the workings of the application procedure. The constraints we have encountered in this regard have alerted us to the impossibility under the present law of any thorough review of the quality of the documentation which is prepared by agents of the Solicitor General — or, for that matter, of the provincial attorneys general. Similarly, the prohibition against disclosure of the content or purport of an intercepted communication, found in section 178.2, has exceptions (such as the giving of evidence in court, or for the purpose of a criminal investigation, or where disclosure is made to a peace officer and is intended to be in the interests of the administration of justice), but they would not permit any independent review of the benefits of interceptions compared with the expectations described in the affidavits. In Part X, Chapter 5 we shall make a recommendation concerning independent review of the authorization procedure, and we shall recommend an amendment to section 178 to permit that review process to have access to the information it would need.

E. NEED AND RECOMMENDATIONS — BRIEF SUMMARY

112. In this Chapter we have, in the course of giving the history and discussing the legal issues, recognized the need for the use of electronic surveillance in both security intelligence collection and criminal investigations. We have also pointed to a number of deficiencies in the law which will be the subject of recommendations in Part V, Chapter 4 and Part X, Chapter 5.

CHAPTER 4

MAIL CHECK OPERATIONS — SECURITY SERVICE AND C.I.B.

A. ORIGIN AND NATURE OF PRACTICE — SECURITY SERVICE AND C.I.B.

1. Research carried out by us discloses that the interception of mail was a matter of concern at least as early as the 1914-18 war. The War Measures Act included a prohibition against dissemination of treasonable material or the passing of information to the enemy. At the beginning of the war a number of postmasters were simply handing over any mail they considered suspicious to the then Royal North-West Mounted Police. It was soon realized that more proper authorization was required and warrants were then obtained under what was then section 629 (now section 443) of the Criminal Code — the section that provides for a search warrant being issued by a justice of the peace. The Post Office Department objected that this was contrary to what was then section 84 of the Post Office Act. The problem was resolved by the senior law officers of the Crown directing that in cases of suspicion the police were to contact senior authorities at the Post Office who would make the necessary arrangements in a proper case. This pragmatic solution continued for some time after the war.

2. The question again became important just prior to the 1939-45 war. By this time the Intelligence Section of the R.C.M.P. had been formed. In early 1939, at about the time the Official Secrets Act was being introduced with a view to meeting the anticipated problem of espionage activity, the Force suggested that the Post Office Act should be amended to permit mail examination in order to counter suspected espionage. Consideration of this suggestion was shelved when the war commenced and the Defence of Canada Regulations brought postal censorship into effect. This solution lasted until the expiry of the regulations in 1954.

3. In late 1954 correspondence and discussions took place between the Force and the Department of Justice with a view to regularizing covert inspection of mail. The Security and Intelligence Special Branch of the R.C.M.P. considered such inspection necessary for security reasons. The possibility of using warrants under section 11 of the Official Secrets Act was considered in view of the fact that the offence created by section 55 (now section 58) of the Post Office Act applied only to a "person who *unlawfully* opens... any post letter, or other article of mail...". At the time, however, it was pointed out that in 1950 section

41 (now section 43[1]) had been introduced into the Post Office Act. It provided as follows:

> Notwithstanding anything in any other Act or law, nothing is liable to demand seizure or detention while in the course of the post, except as provided in this Act or the Regulations.

Consideration was given to amending the Post Office regulations to permit covert examination of mail but nothing came of this suggestion.

4. In October 1957, the Report to the Prime Minister of the Committee of Privy Councillors Appointed to Inquire Into the Interception of Communications[2] (the Birkett Report) (Ex. B-14) was published in the United Kingdom. This report examined the legal authority for the interception of mail, telegraph and telephone communications as well as the purpose, use and extent of the power to intercept, and it made recommendations for the future use of the power. In the United Kingdom all three methods of communication were in fact services provided by the Post Office. The Birkett Committee found that, although apparently originally based upon Crown prerogative, the power to intercept communications in the course of post had been recognized by statute in the U.K. for more than 200 years. Prohibitions similar to that found in section 43 of the Canada Post Office Act had been subject to express exception from 1710 onwards, permitting the interception of mail and, later telegraph on the basis of a warrant of a Secretary of State. The Committee recommended a clarification of the statutes regarding the power to intercept telephone communications. Upon reviewing the use of the power to intercept, the Committee concluded that it had been effective and, subject to continued safeguards, should be continued, since the interference with the individual liberty of law-abiding citizens was relatively small.

5. In Canada, on March 1, 1962, the Director of Administration of the Post Office issued a Directive, addressed to the Regional and District Directors and Senior Investigators, entitled "Narcotics in the Mails" (Ex. B-49). It directed that the Post Office should extend every possible co-operation to the R.C.M.P. in their drug investigations despite the fact that the newly enacted Narcotics Control Act did not override the Post Office Act, which provided (and still provides), that nothing is liable to demand, seizure or detention while in the course of post. The procedure to be followed was not set out but rather left to the discretion of senior officers in the field. The existence of mail suspected of containing narcotics was to be communicated to investigating police in such a way as to inform them of "the precise method, time and place of its delivery to the addressee or of its return to the sender". The co-operation of Customs was to be enlisted in the case of international mail. It was also specified that those in the field did not need to report to Headquarters.

6. This Directive was withdrawn in 1972, when the Department was reorganized on a regional basis, and was subsequently replaced by a Directive dated January 14, 1974, sent by Mr. P. Boisvert to the four Regional Chief

---

[1] R.S.C. 1970, ch.P-14.

[2] Cmnd. 283.

Inspectors of Security and Investigations (Ex. B-51). This Directive specified that because of section 43 of the Post Office Act and other factors, inquiries from R.C.M.P. Drug Enforcement Branch personnel should be directed to Security and Investigations personnel, preferably postal inspectors, rather than the regular Post Office operational staffs. The postal inspectors were briefed on this subject at a postal inspectors' training course held in October 1973, and the issue of special relations with the Post Office was to be included in training courses of R.C.M.P. Drug Enforcement Branch personnel. The January 14, 1974 Directive, and the understanding contained therein, was renewed in an exchange of correspondence dated April 1, 1977 and subsequently confirmed again by letter of January 6, 1978 from Mr. Boisvert to this Commission.

7. Mr. Boisvert told us that it was his clear understanding that any mail cover check operation (that is, the examination of only the outside of a piece of mail) would be done (a) in the Post Office and (b) without removing the piece of mail from the post office where it was located.

8. Documents before the Commission indicate that consideration was given in 1973 to expanding the Protection of Privacy Bill to include specifically the interception of communications by mail. Nothing, however, came of this suggestion.

9. The escalation of drug trafficking in the late 1960s and early 1970s made the criminal investigations side of the Force more anxious to secure legal authority to open mail. Interdepartmental meetings at the instance of the R.C.M.P. began in 1974 with a view to securing appropriate amendments to the Post Office Act.

10. In the summer of 1976, the Security Service attempted to secure access to first-class mail under a warrant which was issued by Mr. Allmand pursuant to section 16 of the Official Secrets Act. He issued the warrant subject to receipt by the Security Service of an opinion that such a warrant was legal. Having been advised by the Department of Justice that section 43 precluded the exercise of such a warrant, the Security Service joined the C.I.B. in seeking amendments to the Post Office Act.

11. Legislation patterned upon the Protection of Privacy Act, which would have amended the Criminal Code, the Crown Liability Act and the Post Office Act, was introduced as Bill C-26 on February 7, 1978, while our hearings relating to Mail Check Operations were underway. This proposed legislation provided for its automatic termination one year after the publishing in the House of Commons of the final Report of this Commission. The Bill perished with the prorogation of Parliament in May 1979, and has not been re-introduced.

B. R.C.M.P. POLICIES AND PROCEDURES — SECURITY SERVICE AND C.I.B.

(a) *Security Service*

12. Although it is apparent from the record before us that mail check operations under the code name CATHEDRAL were carried out by members

of the Security Service from the demise of the Defence of Canada Regulations in 1954, the investigation and evidence before us concentrated on the period from 1970 onward. The principal reason for adopting this time period was that before November 2, 1970, decisions with respect to the use of mail check operations were made by area commanders at the division level, and no records were kept at Headquarters.

13. On November 2, 1970, a senior R.C.M.P. officer sent a memorandum to the commanding officers of the various area commands of the Security Service. The memorandum describes the three types of CATHEDRAL coverage as follows:

> *CATHEDRAL "A" — Routine name or address check* (It was explained in evidence that in this instance, a member of the R.C.M.P. asked a postal employee to record in longhand the name of the addressee and any information with respect to the sender by looking at the outside of envelopes.)
>
> *CATHEDRAL "B" — Intercept (photograph or otherwise scrutinize by investigator) but do NOT open*
>
> (In this instance the same procedure was followed as that in Cathedral "A" but a photographic copy was made of the outside of the envelope. It was explained in evidence that this procedure was used to examine mail covers for simple codes and the possible presence of micro-dots.)
>
> *CATHEDRAL "C" — Intercept and attempt content examination*

14. With respect to authorizing such operations the memorandum directed that Cathedral "A" and Cathedral "B" could be authorized by the local officer in charge, Security and Intelligence Branch, or his designee, but continued: "Because of the special experience required to handle a Cathedral "C" and for this reason only the D.S.I.'s authorization for an operation will henceforth be required. This authority will be contingent on the importance of the case and the availability of a trained technician". The reason given for this change in authorization procedure shows a very clear understanding on the part of the senior officers at Headquarters as to the legality of such techniques. The first two paragraphs of the memorandum read as follows:

> *Re: CATHEDRAL*
>
> It has become apparent that considerable diversity exists in the understanding and the utilization of this source and that we are unconsciously exposing this source's availability to unwarranted risk. Since this source is extremely valuable, perhaps in regard to counter-espionage particularly, it has been decided that there should be some uniformity brought into the picture by outlining guidelines which will create as few restrictions and limitations as possible and still effectively reduce the risk.
>
> It must be clearly understood that any form of co-operation received from any CATHEDRAL source is contrary to existing regulations. There is absolutely no indication that this aspect is likely to be rectified in the near future. Since these investigations involve National Security, it is considered there is a sufficient element of justification to proceed with the development and cultivation of sources who are willing to co-operate on this basis. Each source who co-operates with the Force is actually risking his livelihood and

this fact must be kept in mind when the individual is being recruited or subsequently handled.

Directions were given in the memorandum as to co-ordinating and supervising the operation at each of the divisions. Concern was expressed that all approaches to Post Office personnel should be co-ordinated and that liaison should be maintained between the Security Branch and the C.I.B. "to ensure there is no conflict".

15. It may be noted that, although from late 1970 onward policy required that all Cathedral "C" Operations be approved by Headquarters, there were Cathedral "C" operations in nine cases from 1971 to 1976, without approval having been obtained (Ex. B-31).

16. A former senior R.C.M.P. officer testified that Cathedral "C" was in fact used in cases of counter-terrorism, counter-espionage and later to protect persons against letter bombs. He knew of no other areas of activity in which authorizations were granted in the Security Service for a Cathedral "C" operation.

17. In the late spring of 1973 an incident occurred in connection with mail service which caused an addressee to communicate with Members of Parliament regarding the opening of mail. Because Headquarters was concerned that this might result in public revelation of the Cathedral operations, a message was sent on June 22, 1973 (Ex. B-17), to all Area Commanders which directed that:

> All Cathedral "A", "B", and "C" operations are to be suspended until further notice. No further operations are to be instituted until you are advised the suspension is lifted.

18. No record or instruction has been found to indicate that there was ever a formal revocation of the suspension of Cathedral operations directed in the telex of June 22, 1973. However, subsequent evidence (*in camera*) indicates that one Cathedral "C" operation was authorized in September 1973 and a number were approved in 1974 (Exs. BC-2, BC-3, and B-31).

19. Assistant Commissioner M.S. Sexsmith was in security and intelligence work in the R.C.M.P. from 1958 until January 1978. In May 1973, he was the Area Commander of the Security Service in Toronto. In August 1975, he became Deputy Director General (Operations). He indicated to us that upon his appointment as "D.D.G. Ops" he adopted a policy pursuant to which he had not seen fit to authorize any Cathedral "C" operations. The reasons given by him for not authorizing any Cathedral "C" operation from the time of his appointment on August 1, 1975 may be summarized as follows:

(a) The American experience with Watergate and the suspicion of the media in Canada that there was a Watergate in this country might lead to disclosure of the mail examinations and interceptions and thus cause damage to the Security Service.

(b) Some former members of the R.C.M.P. were beginning to talk to the media and "other people".

(c) Several initiatives over a long period of time to have the law amended so that the mail could be opened legally "under strict control" had failed and it seemed, to Mr. Sexsmith, to be unfair in the circumstances to ask members of the R.C.M.P. "to stick their necks out and open mail".

20. An incident involving a mail-cover check in the Hamilton area first came to public attention on November 8, 1976, when Mr. Paul Boisvert, Director of Security and Investigations in the Post Office, received information from the Postmaster General's Office to the effect that a complaint had been received concerning a mail check in Hamilton. Mr. Boisvert immediately telephoned the Regional Chief of Security and Investigations and requested him to conduct an investigation. The investigation disclosed that on or about October 4, 1976, a postal inspector in Toronto received a request from the R.C.M.P. to implement a mail-cover check on a subject living in Hamilton. The Toronto postal inspector sent a memo to the manager of the Hamilton post office requesting that mail addressed to the subject be sent under registered cover to the Toronto unit.

21. "Approximately 30 pieces of sealed letter mail" were received by the postal inspector in Toronto, where these letters were photostated and returned the same day, again under registered cover, to the Hamilton post office. None of the envelopes was opened or left the custody of the Post Office (Vol. 17, p. 2638). In one case the postal inspector remembered one small sealed envelope having arrived at the Toronto office repaired with scotch tape on the centre of the cover. According to the postal inspector this was returned in the identical condition.

22. The postal inspector added in his report to the Chief Postal Inspector of the Ontario postal region that in the past he had complied with similar confidential requests "placed with (his) unit, by special law enforcement squads". He further pointed out that this type of co-operation was suggested in his Investigator's Manual, and that the R.C.M.P. officers involved in the matter never took possession of the mail, did not open or damage any articles, and did not disclose the purpose of the investigation.

23. Mr. Boisvert met with the Postmaster General on November 16, 1976 at which time he assured the Minister that "this was an isolated incident that was improperly handled by the postal inspector who was due to retire next month". However, he was satisfied that "the mail never left the custody of the Post Office", and, further, that he had met with senior officials of the Royal Canadian Mounted Police who assured him "that they did not come into possession of the mail as for their purpose they were satisfied with the photocopies of the outside of the envelopes only". While he felt that the action requested by the R.C.M.P. in that instance was justified, "in view of the national and international implications" it was regrettable that the postal inspector did not deal with the matter "more intelligently". It was Mr. Boisvert's opinion that the postal inspector in Toronto should not have written a memo to Hamilton, and that the mail should not have been directed from Hamilton to Toronto and back to Hamilton. Mr. Boisvert assured the Minister that he was taking measures to avoid such incidents in the future.

24. As a result of this incident, on November 18, 1976, Mr. Boisvert met with the Deputy Director General (Operations) and the officer in charge of the Sources Branch concerning R.C.M.P. requests for Post Office co-operation and assistance in matters relating to the national security of Canada. It was decided at the meeting that any requests from the R.C.M.P. for special investigations of the mail in cases where it was considered "in the best interest of Canada and the public", would be funneled through the Ottawa offices of the Security and Investigation Services Branch. The decision as to whether co-operation should be extended by the Post Office would be made by Mr. Boisvert as the Director of Security and Investigation Services, or by the Chief of Investigations. If it were decided that co-operation was to be extended, the Regional Chief Inspector would be contacted and instructed accordingly. R.C.M.P. field units were not to seek assistance at the local levels, and any such requests were not to be accommodated.

25. In Mr. Boisvert's letter to the Regional Chief Inspector, he confirmed that "under no circumstances will the Canada Post Office permit mail to be illegally opened, delayed, tampered with or be removed from our premises". The R.C.M.P. report of this meeting is dated November 22, 1976, signed by Assistant Commissioner M.S. Sexsmith as Deputy Director General (Operations), and sent to all Divisions. Assistant Commissioner Sexsmith's guidelines, as sent out to the field correspond to the guidelines sent by Mr. Boisvert to the field.

26. From and after November 22, 1976, approval for all Cathedral operations was centralized at Headquarters, (Ex. B-20). At the same time area commanders were advised of the new policy which required that, instead of field units making arrangements with local post office people, all requests for Cathedral operations were to be sent to Headquarters for approval by either the Director General or the Deputy Director General (Operations). Assistant Commissioner Sexsmith testified that, while he had not authorized any Cathedral "C" operations since August of 1975, he had approved several Cathedral "A" and "B" operations.

27. Although Assistant Commissioner Sexsmith had not authorized any Cathedral "C" operation since August 1, 1975, he became aware, as a result of research undertaken in the R.C.M.P. in preparation for his appearance before us, that during 1976 a "local initiative" by a member or members of the Security Service had resulted in the opening of two letters in the OMURA case in Toronto. This case is dealt with in some detail in Part V, Chapter 4.

28. In addition, Assistant Commissioner Sexsmith testified that in July 1976 he was told of an operation in Ottawa by a member of the Security Service which was directed against foreign intelligence officers. Approval for the operation had been given in 1975. During the operation, on three or four occasions a letter posted was retrieved by members of the Security Service while it was in the course of the post. Assistant Commissioner Sexsmith gave instructions to cancel the operation, and it was stopped in July 1976.

29. Apart from the two incidents mentioned above, Assistant Commissioner Sexsmith believed, at least until the detailed review undertaken for the

purposes of the Commission, that the policies he introduced in August 1975, had been followed in the Security Service. However, it is apparent that two additional Cathedral "C" operations were approved at the divisional level during 1976 in direct violation of the formal policy of the Security Service.

30. In September 1977, the officer in charge of the Legal Branch of the R.C.M.P. was asked to consider the effect of the Post Office Act on mail check operations. He consulted with the legal adviser to the Post Office Department and in a memorandum (Ex. B-21) stated that it was illegal for anyone to open and examine mail with or without the co-operation of the postal authorities at any time after posting and before delivery. He also stated that he was not aware of any regulations or postal policy restrictions which would prevent the R.C.M.P., with the co-operation of the postal authorities, from viewing or photographing (not x-raying) any specific items of such *en route* mail. He cautioned, however, that care should be taken that any such mail not be detained.

31. As a result, on September 23, 1977, Headquarters sent a message to all area commanders (Ex. B-22), which quoted the text of the memorandum, and continued:

> ...It is emphasized that a Cathedral "B" operation must not go beyond examination of the outside of mail... Cathedral "A" and "B" requests will continue to require Director General or Deputy Director General (Operations) approval. As has been the practice in recent years Cathederal "C" requests will not be considered.

32. Assistant Commissioner Sexsmith, testifying before us in December 1977, said that the message set out the current policy and procedure of the R.C.M.P. Security Service.

33. After the question of mail check operations had become a matter of public discussion as a result of a television programme broadcast on November 8, 1977, Assistant Commissioner Sexsmith sent a directive, dated November 21, 1977, to area commanders, which he said resulted from the knowledge which he had recently acquired, that in "very few instances" after he began his term of office on August 1, 1975, Cathedral "C" operations had occurred without the approval of Headquarters. The message (Ex. B-23), states:

> It is therefore necessary to make clear that all Cathedral operations with the exception of the Cathedral "A" category, will not be entertained under any circumstances. As a result of discussions with postal authorities, it has been agreed that they will continue to co-operate on Cathedral "A" requests which are not illegal. There is one important stipulation to the effect that mail must not leave postal premises and must not leave the possession of postal authorities. Mail covers may be photographed or photocopied provided secure facilities are available on post office premises, but again under no circumstances is mail to be removed from postal premises nor is it to be delayed for any reason.
>
> This policy must not be abrogated for any reason whatsoever. Regardless of the rationalization, no deviation however slight, shall be tolerated. It will be the duty of every area commander to ensure that this policy is strictly adhered to.

> Please ensure that Cathedral "A" requests are fully supported with complete rationale when seeking authorization.

This directive was in its essentials the same as the message of September 23, 1977.

(b) *Criminal Investigation Branch*

34. A review of the use of mail check operations in criminal investigations by the R.C.M.P. was more difficult than the review of the use of such techniques by the Security Service because the C.I.B. did not have any centralized system of authorization or record keeping. It was apparent, however, that mail check operations became increasingly important to the C.I.B. in the late 1960s and 1970s because of increasing use of the mails for the importation and distribution of drugs.

35. Policy with respect to the subject was dealt with in successive issues of the R.C.M.P. Operations Manual. The earliest Manual page that could be located that dealt with this matter was dated June 15, 1972 (Ex. B-27).

> Section 41 of the Post Office Act protects mail in transit from seizure, except under the Customs Act. When you wish to search postal premises, consult with the senior local representative of the Post Office Department and arrange a postal inspection as postal officials are given additional powers under the Act.

Since February 1973 the Manual has contained more detailed instructions.

36. In December 1973 the Director of Criminal Investigations sent a memorandum (Ex. B-28), to the commanding officers of the various divisions concerning "Co-operation with the Post Office Department". After quoting what is now section 43 of the Post Office Act he said:

> The Postal Department does not wish to jeopardize the co-operation which presently exists between their investigators and our members, nor restrict our drug investigations in any way. However, when it is anticipated during an investigation that the Post Office co-operation will be brought out in court proceedings the following policy is to be adhered to:
>
> > Parcels or letters committed to the mail service will not be opened nor the contents interfered with, except during Customs examinations. To determine that a parcel originating in one area of Canada is the same parcel which is received and delivered at some other location in this country... (this was followed by a description of the technique).

37. At the time of the hearings before the Commission the instructions to the Drug Enforcement Branch were given by a bulletin (Ex. B-29), from the C.I.B. Directorate at Headquarters reminding members of the Force that in investigating illicit use of the mail system they were to "ensure that [they] are familiar with the Post Office Act and particularly s.43 and 46". At the time of the hearings before us in December 1977, a new memorandum of instructions was in the course of preparation.

C. EXTENT AND PREVALANCE OF THE PRACTICES

—

SECURITY SERVICE AND C.I.B.

(a) *Security Service*

38. A detailed review of the records of the Security Service was undertaken to determine the extent and prevalence of Cathedral operations during the period from November 1970 to the end of December 1977. A total of 94 mail check operations were identified of which 66 involved the actual opening of mail (Cathedral "C") and in two more cases opening was authorized but not carried out. Of these 66 cases, 21 occurred in the period of 1970 to 1973 in Quebec and were related to persons known or suspected to be involved in F.L.Q. terrorist activities. Another 11 related to persons known or suspected to be involved in international terrorism. Suspected espionage activities and foreign interference in Canadian political affairs accounted for 25 more cases, and there were nine miscellaneous targets.

39. The examination of the exterior of envelopes without photographing them (Cathedral "A") occurred in six cases, of which four related to suspected international terrorists, and two related to suspected or known espionage.

40. The examination and photographing of the exterior of envelopes (Cathedral "B") occurred in 19 cases and was authorized but not carried out in one other case. Of these 20 cases, 11 related to suspected international terrorists, and nine related to suspected or known espionage.

41. The Post Office Department also conducted several surveys at the Commission's request. In November 1977, the Post Office conducted a telephone survey across the four regions, Atlantic Region, Quebec, Ontario and Western Region. Subsequently, Post Office officials conducted interviews with 79 postal inspectors across the country. This series of interviews related to the relationship of the Post Office specifically with the Security Service of the R.C.M.P., rather than with the entire Force.

42. Of the Post Office surveys, the first survey, conducted over the telephone on November 9, 1977, was intended to ascertain what knowledge the regional Chief Inspectors had of the degree and number of requests which might have been made to the Post Office by the R.C.M.P. for either the opening of mail, or mail cover checks, for the period of November 1976 to November 1977. The results were as follows:

(a) Response from the Atlantic region indicated that although there were some local contacts prior to 1976, the two requests originating from the R.C.M.P. in the one-year period from November 1976 to November 1977 were both turned down by the Post Office.

(b) The Ontario region advised that it had received several requests through the Ottawa office during that year, and that there had been local contact prior to November 1976. According to the information provided by the Chief Inspector of the Ontario postal region, no mail was ever turned over

to the R.C.M.P., and no cover checks carried out, though mail covers may have been photocopied in the Ontario region Security and Investigation office.

(c) Quebec postal region office was aware of several requests since November 19, 1976, as well as some local contact prior to that time, but it maintained that no mail had ever been turned over to the R.C.M.P.

(d) As far as the Western region was concerned, some requests had been made for mail cover checks before November 19, 1976. No further requests were made after that date. Also, no mail was handed over to the R.C.M.P., or left the Post Office.

43. Post Office officials then conducted a more detailed interview survey of postal inspectors, past and present, from across the country. Selection of the postal inspectors was based on R.C.M.P. Security Service statistics which indicated where, according to their records, mail may have been opened in the course of Cathedral "C" Operations. At that time Security Service statistics pointed to 70 Cathedral "Cs", and therefore an effort was made to interview 79 postal inspectors. Forty of the inspectors interviewed indicated that they were never involved in any opening of the mail. Of the remaining 39 inspectors, 32 were current inspectors at the time of the interviews, and seven were former inspectors. Of the 32 current inspectors, two had given verbal statements to the Minister on November 16, 1977. One other refused to give a statement, another two were on sick leave at the time, and three others were not interviewed because they were not employed in the relevant area at the relevant time. One said orally that he had no involvement but refused to give a statement in writing, seven stated they were not involved because they were not present at the time and place suggested. The remaining group of 16 was not interviewed because information from the R.C.M.P. was that, although authorization to open mail had been granted, the procedures were not implemented; therefore no mail was opened in those instances. Of the seven former inspectors, two could not be located because their addresses were unknown and five refused to give statements.

(b) *Criminal Investigation Branch*

44. It was not possible to determine the extent and prevalence of mail check operations of the C.I.B. from centralized records, nor were the various types of check neatly classified by any code names such as Cathedral "A", "B", and "C". Because the interest of the C.I.B. arises particularly from the use of mails for the importation or distribution of drugs, the C.I.B. used the additional technique of "controlled delivery". Two instances, cited to us, in which this technique was employed, were (a) the receipt of advance information from foreign countries indicating that as many as 260 letters containing drugs would be arriving in the course of mail, and (b) Customs examination of packages disclosing the presence of drugs. In such circumstances members of the R.C.M.P. might participate in the delivery of mail to assist in the apprehension of the intended recipients after delivery is clearly established and before the drugs are put in circulation (Vol. 8, pp. 1119-20).

45. An attempt was made to have local divisions check for mail intercepts of all kinds. The results are summarized in Exhibit B-84 and in the evidence of Assistant Commissioner Venner (Vol. 18, pp. 2802-19). From this it will be seen that the vast majority of incidents related to enforcement of the laws concerning drugs. The difficulties occasioned by the definition of "letter", "first-class mail", "post letter" and "delivered" as discussed later in this chapter make the results questionable. Nevertheless, the following points are clear concerning the years 1970 to 1977:

(a) There were 954 mail intercept operations.

(b) Of these, 799 involved the opening of pieces of mail.

(c) Of the 799 cases, 100 involved mail within the dictionary definition of "letter", being "a written or typewritten communication on a piece of paper". The remainder (699) fell within the post office's broader definition of "post letters".

In addition, 592 pieces of mail were examined externally, and 258 pieces of mail were delivered under controlled circumstances.

46. These statistics provide a general indication of the extent and prevalence of mail openings and mail check operations on the criminal investigation side of the Force. They also show a great variance in different parts of the country in the interpretation and application of provisions of the Post Office and Customs Acts. It may be noted that there were no reported instances of C.I.B. mail interception in Quebec in search of either drugs or other substances. The explanation provided by "C" Division in Montreal for their statistics, which indicate that no mail was opened, rested on their position that anything other than "a simple envelope with obvious written communication inside is not first-class mail, regardless of the postage paid on it", and it was felt that it was not improper to open such other mail.

47. Assistant Commissioner T.S. Venner testifying before us on February 1, 1978, said that the postal customs authorities in Montreal were and are

> much more active in the opening of mail. . . than they are anywhere else in Canada. Our people simply found it necessary to get that involved. They rely on the postal customs people to alert them as to what they have found, and, in some cases, put the material back in the system for control and delivery and the openings are not done by our people.
>
> (Vol. 18, p. 2803.)

(Assistant Commissioner Venner subsequently informed us that he believes he said "unnecessary", not "necessary". We are satisfied that whatever he said, he clearly meant "unnecessary".) He explained also that another reason for non-activity by members of the drug section in Montreal in opening mail is that they "are not usually working on the kind of international cases which involve the smuggling of quantities of heroin by mail" but on importation cases which involve the use of couriers.

48. In contrast, in Southern Ontario, 389 pieces of mail were opened to determine whether drugs or other substances were contained in them. Of the 389 opened in Ontario, 252 were second or other class mail. It was not clear

what percentage of the remaining pieces of mail were first class. Furthermore, it was not clear how many pieces were opened by Customs and Postal officials, and the suggestion was made that none were opened by the R.C.M.P. but rather they were inspected or seen by the R.C.M.P. after having been opened by persons other than a member of the R.C.M.P. That, of course, is not an end of the legalism, for, if a source in the Post Office undoubtedly opens a letter, he commits an offence under section 58 of the Post Office Act; and a member of the R.C.M.P. who encourages him to do so is a party to the offence by virtue of section 21 of the Criminal Code. The offence depends on the opening being "unlawful" and that element of unlawfulness might be satisfied by the fact that the postal employee may have committed an offence under section 387(1)(c) of the Criminal Code ("Everyone commits mischief who wilfully... (a)... interferes with the lawful use, enjoyment or operation of property") or at least the tort of conversion. Vancouver was the other city which showed a large number of pieces of mail opened in the search for drugs: 406 pieces of mail were intercepted in search of drugs and five pieces of mail were intercepted in the search for other material.

49. In order to examine the extent and prevalence of mail intercept and mail opening practices by the R.C.M.P., it was necessary, in addition to the general statistics, to look at what might be involved in any single Cathedral or Mail Intercept Operation. One Cathedral Operation may involve numerous pieces of correspondence that are either checked on the cover or opened. The Commission heard evidence on behalf of both the Security Service and the Criminal Investigation Branch concerning specific examples of Mail Opening or Cathedral Operations. In the OMURA Case, presented by the Security Service, there were two instances of mail opening not authorized by Headquarters out of 50 items of mail examined.

50. On the criminal investigation side of the Force, eight cases were reviewed publicly and in each case some of the parcels were opened either while in the course of post, or after delivery. In most cases the openings were of international mail by Customs officials, with R.C.M.P. officers assisting or taking over for controlled delivery procedures.

D. LEGAL AND POLICY ISSUES — SECURITY SERVICE AND C.I.B.

Statutory provisions

51. The following are the relevant provisions of the Post Office Act.

(a) A definition of ownership of the mail is found in section 41:

> 41. Subject to the provisions of this Act and the regulations respecting undeliverable mail, mailable matter becomes the property of the person to whom it is addressed when it is deposited in a post office.

Thus an addressee has a property interest in mail once it is deposited in a post office. Consequently, any tampering with it is in some sense unlawful unless it is done by consent of the addressee or by statutory provision.

(b) A prohibition against "demand, seizure or detention" is found in section 43:

> 43. Notwithstanding anything in any other Act or law, nothing is liable to demand, seizure or detention while in the course of post, except as provided in this Act or the regulations.

This is the section which overrides search warrants under the Criminal Code or ministerial warrants under section 16 of the Official Secrets Act.

(c) Sections 58 and 59 create offences. Of these, section 58 is the more important for our purposes, as it makes it an indictable offence to delay or detain any article of mail unlawfully, or to open it or suffer it to be opened unlawfully:

> 58. Every person is guilty of an indictable offence who unlawfully opens or wilfully keeps, secretes, delays or detains, or procures, or suffers to be unlawfully opened, kept, secreted, or detained, any mail bag, post letters, or other article of mail, or any receptacle authorized by the Postmaster General for the deposit of mail, whether the same came into the possession of the offender by finding or otherwise.
>
> 59. Every person is guilty of an indictable offence who abandons, obstructs or wilfully delays the passing or progress of any mail or mail conveyance.

52. There are only two exceptions to section 43 in the Post Office Act. The first exception, found in section 7, allows the Postmaster General to detain mail, and in certain cases, forward it to a Board of Review that may open and examine it "with the consent of the person affected". The requirement that notice be given to the person affected renders this section inappropriate for criminal or security investigations.

53. The second exception is found in section 44 (formerly 46) which empowers Customs Officers to examine international mail, and provides in subsection 2:

> (2) A customs officer may open any mail, other than letters, submitted to him under this section, and may
>
> (a) cause letters to be opened in his presence by the addressee thereof or a person authorized by the addressee; or
>
> (b) at the option of the addressee, open letters himself with the written permission of the addressee thereof;
>
> and where the addressee of any letter cannot be found or where he refuses to open the letter, the customs officer shall return the letter to the Canada Post Office and it shall be dealt with as undeliverable mail in accordance with the regulations.

A member of the R.C.M.P. becomes part of this process by virtue of section 17(4) of the R.C.M.P. Act, which states as follows:

> (4) Every officer, and every member appointed by the Commissioner to be a peace officer, has, with respect to the revenue laws of Canada, all the rights, privileges and immunities of a customs and excise officer, including authority to make seizures of goods for infraction of revenue laws and to lay informations in proceedings brought for the recovery of penalties therefor.

Further, the Customs Act,[3] in section 2(1) defines officer as:

> ...["officer" means] a person employed in the administration or enforcement of this Act and includes any member of the Royal Canadian Mounted Police;

Effect of section 43 on section 16 of the Official Secrets Act

54. Section 16(2) of the Official Secrets Act provides that:

> (2) The Solicitor General of Canada may issue a warrant authorizing the interception or seizure of any communication if he is satisfied by evidence on oath that such interception or seizure is necessary for the prevention or detection of subversive activity directed against Canada or detrimental to the security of Canada or is necessary for the purpose of gathering foreign intelligence information essential to the security of Canada.

55. On the face of it, "any communication" would seem to include postal or written communication. As has already been recounted, Mr. Allmand signed a warrant in 1976 authorizing the interception of written communications subject to an opinion from the Department of Justice. The opinion, however, indicated that even though the word "communications" was seen by the Department of Justice as including letters, the wording of section 43 of the Post Office Act was so clear as to preclude section 16(2) of the Official Secrets Act from enabling the opening of letters in the course of post.

56. In Chapter 3 of this Part, where we discussed in detail the legal issues relating to Electronic Surveillance, we considered whether section 16(2) is, in our view, available at all in respect of letters. In section E of this chapter, and more fully in Part V, Chapter 4, we make recommendations as to the circumstances and conditions in which the opening of mail should be permitted in security matters.

International mail

57. It will be recalled that, pursuant to section 46(2) of the Post Office Act, a Customs Officer (which, pursuant to the Customs Act, includes any member of the R.C.M.P.) may open any mail *other than letters*. However, the Post Office Act does not contain a definition of "letter". It does contain, in section 2(1), a definition of "post letter":

> "post letter" means any letter deposited at a post office, whether such letter is addressed to a real or fictitious person, is unaddressed, and whether intended for transmission by post or not, from the time of deposit at a post office to the time of delivery and includes any packet prepaid or payable at letter rate of postage;

It will be observed that the definition appears to be intended to be broad in scope. In the absence of a statutory definition, the dictionaries tell us that a "letter" is a "written or printed message addressed to person(s), usually sent by post or messenger and fairly long" (Concise Oxford Dictionary); "a direct or personal written or printed message addressed to a person or organization"

[3] R.S.C. 1970, ch.C-40.

(Webster's New Collegiate Dictionary). There do not appear to be any Canadian judicial decisions interpreting "letter", but in the United States the word has been construed as meaning "a communication in writing from one person to another at a distance, and a written or printed message".[4]

58. The evidence before us has shown that at least in one major point of arrival for international mail there is a narrow interpretation of "letters" as that word is used in section 46(2) by Customs officials. In Montreal they feel free to open all international mail except "a simple envelope with obvious written communication inside", (Vol. 18, p. 2803). If this interpretation were used in all centres, there would be no impediment to the opening of any envelope or packet in "international mail" that appears to contain something other than a "written communication". However, the Montreal interpretation is not common, and therefore the Customs officials and R.C.M.P. in other centres are constrained not to open mail that would be opened in Montreal, although we do not have clear evidence as to the criteria used elsewhere.

59. The confusion becomes compounded when it is realized that, under the Post Office International First Class Mail Regulations,[5] "first class mail" is defined as including not only letters and postcards in handwriting or typewriting but also *any* item of mail that the sender chooses to prepay at first class rates. Thus parcels as much as one cubic foot in size might, pursuant to the size and weight limitations contained in those regulations, be "first class mail" if there is first class postage prepaid. We note this simply because so many news reports have spoken of the legal issue as being whether the R.C.M.P. or a postal employee may lawfully open international "first class mail". In fact, as we have seen, section 46(2) empowers customs officers to open *any* mail, of whatever class, without the addressee being present or having given his permission — except in the case of "letters". Consequently, while we have noted the international first class mail regulations, we do not believe that they are relevant to the legal problem.

Domestic mail

60. We turn now from international mail to domestic (solely within Canada) mail and all mail from abroad or addressed to a foreign destination while it is in the course of post in Canada. The prohibition contained in section 43 applies to all these kinds of mail: it is not subject to "demand, seizure or detention". Moreover, under section 58, it is an indictable offence to open any "article of mail" unlawfully or wilfully to "delay" or "detain" it. The "unlawfulness" of opening mail as such is found in a breach of the prohibition contained in section 43. We now apply those provisions to several possible domestic situations.

(a) Examining the exterior of an envelope (what the Security Service has called Cathedral 'A') might be unlawful if the length of time it is taken out of the mail stream results in its being "detained" or "delayed". Even if

[4] *Buckwald* v. *Buckwald*, 199 A. 795 at 799, 175 Md 103.
[5] S.O.R./71.336.

that were not so on the facts of most situations, it might be argued that a civil wrong is committed by interfering in the ownership of the article of mail, but this is doubtful. On balance, we do not believe that this investigative practice, if it does not involve removing the article from the mail stream for any significant length of time, can be said to be an activity "not authorized or provided for by law". This is particularly our view if the article of mail remains at all times in the control of a postal employee. Our view is the same as that of the Director of the Legal Services Branch of the Post Office, given in December 1977. Nevertheless, as will be seen, we consider that this technique involves such a degree of intrusion into the privacy of the persons involved that a higher level of approval of such an operation should be required than has been so in the past.

(b) The same remarks apply to photographing the exterior of an envelope (what the Security Service has called Cathedral 'B').

(c) If a postal employee hands an article of mail to a member of the R.C.M.P. so that he may open and examine its contents, both he and the R.C.M.P. member may be guilty as being accessories under section 58 of opening an article of mail unlawfully. The unlawfulness will lie in wilfully interfering with the lawful use, enjoyment or operation of property, which is mischief under section 387(1)(c) of the Criminal Code, or in the civil wrong of conversion, which involves even a temporary interference with another person's interest in property. Even if there is any doubt about that, the time taken to carry out the operation, especially if the opening is carried out off postal premises, may well constitute wilful delay or detention. Consequently, for one reason or another what the Security Service has called Cathedral 'C' would likely be an offence.

(d) Controlled deliveries: there are several techniques of controlled delivery which must be examined:

(i) The first situation involves the substitution of other innocuous substances for most of the drug found in any one item of mail, leaving only a small part of the original substance. The item of mail is then resealed and placed back in the system for delivery by postal officials. In this case it may be argued that the mail was not detained as long as this procedure was expeditious. Opinions written by legal officers of both the Department of Justice and the Post Office have so indicated. However, the point may also be made that the addressee's property has been tampered with, and that gives rise to the issues of mischief and conversion that have already been discussed, as well as theft.

(ii) The second situation involves the same type of substitution, but the delivery itself is by disguised members of the R.C.M.P. to the addressee's residence, rather than by postal officials. In this case, as in the first, if the procedure is effected expeditiously, it would not appear that section 58 concerning detention of mail is breached. The second point, however, still remains the same; there may have been such tampering as gives rise to issues of mischief, conversion and theft.

(iii) The third situation is exactly the same as the second, with the provision that the delivery to the addressee's residence is made by a disguised officer at a pre-arranged time under surveillance by R.C.M.P. members. This situation would probably involve the detention of mail, depending on the length of the delay involved in pre-arranging the delivery.

(iv) The fourth situation involves removal of an article of mail from the post office premises to an R.C.M.P. laboratory, its being opened there and its being subsequently resealed and returned to the post office for one of the previous three methods of controlled delivery. This clearly results in wilful detention and delay contrary to section 58.

(e) In an examination or photographing of envelopes, or opening an article of mail, before it is deposited in a "post office" (which includes a letter box), nothing is being done to an article in the course of post, and so the Post Office Act is inapplicable. A member of the R.C.M.P. could lawfully employ any of these techniques pursuant to section 10 of the Narcotic Control Act if he has a writ of assistance, the search is not of a dwelling-house, and he reasonably believes the article of mail contains a narcotic. If these conditions are not satisfied, any of these techniques might result in trespass, mischief, or conversion, depending upon the circumstances.

(f) The observations made in (e) apply to the examination or photographing of envelopes, or opening an article of mail, after it is delivered to a locked post office box, apartment box or rural mail box.

(g) In the case of letter bombs, if it is *known* that an article of mail contains an explosive, then the article of mail is considered "non-mailable matter" under sections 1 and 2 and Schedule I of the Prohibited Mail Regulations, and consequently, whether it is domestic mail (section 44 of the Act) or International mail (section 46(4) of the Act), it is to be disposed of by the Postmaster General's Department "in a manner that will not expose postal employees to danger" (section 4 of the Regulations). However, no assistance is provided by the Act or Regulations where there is mere reasonable belief that an article of mail contains a bomb, or only suspicion that it may do so. In such cases it appears that a postal employee or a member of the R.C.M.P. who opens an article of mail commits an offence under section 58, except when the mail is international and the article opened (by a Customs Officer, which includes R.C.M.P. members) is not a "letter".

61. Counsel for the R.C.M.P. suggested to us that the R.C.M.P.'s power to open mail might be available on the basis of the Crown prerogative, but in our view, even if there were some such prerogative power rooted in history, the Post Office Act, by prohibiting demand, seizure and detention in section 43 and thus making opening "unlawful" under section 58 if it involves demand, seizure or detention, has precluded any possibility of sustaining an argument that opening is lawful by virtue of the exercise of a prerogative.

E. NEED AND RECOMMENDATIONS — BRIEF SUMMARY

62. In Part V, Chapter 4, we conclude that the need exists to permit the security intelligence agency lawfully to open envelopes and read messages. However, the use of this technique should be strictly and carefully controlled in individual cases, and the subject of regular and prudent study by the independent review body which we shall recommend be established. The power to use these techniques should be limited to the investigation of espionage, foreign interference and serious political violence.

63. As for the criminal investigation side of the Force, we conclude in Part X, Chapter 5 that peace officers should have the power to examine or photograph an envelope or to open mail only in narcotic and drug cases. This power should be limited to examination and testing of any substance found in the mail. Unless a narcotic or restricted drug is found in the mail reading an accompanying message should be made an offence. Peace officers exercising this power should require a judicial authorization subject to the same safeguards as are now found in section 178 of the Criminal Code governing the use of electronic surveillance.

CHAPTER 5

ACCESS TO AND USE OF CONFIDENTIAL INFORMATION HELD BY THE FEDERAL GOVERNMENT — CRIMINAL INVESTIGATIONS

A. ORIGIN, NATURE AND PURPOSES OF PRACTICES

1. The various departments and agencies of the federal government are a storehouse of personal information about Canadian citizens and others who are required under various statutes to provide that information to the government. This is particularly so with respect to the income tax records of the Department of National Revenue and the employment records of the Canada Employment and Immigration Commission. Access to the government's store of information has a strong attraction for the R.C.M.P., both for their own use and to assist other police forces, at home as well as abroad. In investigating offences, keeping the peace or simply assisting members of the public, the R.C.M.P. need all available sources of information and obviously, the more they have available, the better able they will be to resolve a given problem.

2. On the other hand the government, for several reasons, has felt it advisable to restrict access to personal information provided to it by individuals. In addition to the general reluctance to have the privacy of individuals invaded unnecessarily, the government recognizes the need for confidentiality of tax records if it hopes to operate a tax system which, although compulsory in law, is in reality based on voluntary compliance. The government has also believed that, to obtain public co-operation in a universal social insurance scheme (including manpower and unemployment insurance programmes), it has to provide an assurance that the information received by it will not be disseminated for other purposes. Consequently, many statutes which compel production of such information include restrictions on access to it. The R.C.M.P., in the pursuit of its duties, has breached those provisions either with specific approval from Headquarters, as a Force policy, or with the tacit approval of senior officers. As will be seen in this chapter, this practice of law-breaking became institutionalized within the R.C.M.P.

3. The Criminal Investigation side of the R.C.M.P. has sought access to five distinct sets of government records: the income tax records of the Department of National Revenue, the employment records of the Canada Employment and Immigration Commission (formerly the Unemployment Insurance Commission), the family allowance and old age security records of the Department of

National Health and Welfare, the Industrial Research and Development Incentives Act financial grant records of the Department of Industry, Trade and Commerce and finally the records compiled by the Foreign Investment Review Agency pursuant to the provisions of the Foreign Investment Review Act. We shall now examine those five cases in detail.

B. DEPARTMENT OF NATIONAL REVENUE

Policy and implementation

4. The relationship between the Criminal Investigations (C.I.B.) side of the R.C.M.P. and the Department of National Revenue (D.N.R.) has varied over the years. At present that relationship covers two distinct areas: first, the routine enforcement of the Income Tax Act which includes the location and prosecution of delinquent taxpayers, and second the organized crime Tax Programme (Vol. 47, pp. 7582-3). That programme, which we shall describe in detail later, is an agreement between the R.C.M.P. and the D.N.R. to co-operate in enforcing the provisions of the Income Tax Act against persons described as being involved in "organized crime". We heard considerable evidence as to how different people working on the programme defined "organized crime", but since for the purposes of examining the legality of the actions of the people involved the definition of "organized crime" is not pivotal, we will not examine it other than to quote one definition used by the R.C.M.P.: "two or more persons concerting together on a continuing basis to participate in illegal activities either directly or indirectly for gain" (Ex. G-1, Tab 35).

5. The activities of the R.C.M.P. relating to the routine enforcement of the Income Tax Act include the locating of delinquent taxpayers, laying of informations and complaints, serving summonses and executing warrants of commitment and of arrest, and obtaining search warrants (Vol. 47, pp. 7583-7; Ex. G-1, Tab 3; Ex. G-2 for identification, Tabs 1 and 2). The primary responsibility for enforcement of the Income Tax Act lies with the D.N.R. and the responsibility of the R.C.M.P. in this regard is secondary (Vol. 47, p. 7594). This area of relationship is of long-standing duration and in itself has not given rise to any misconduct which we have been able to uncover.

6. Most of the activities which have been the subject of our concern arose out of what came to be known as the Tax Programme. Prior to 1972 the R.C.M.P. passed information to the D.N.R., through a strictly informal arrangement, about criminals being investigated by the R.C.M.P. (Vol. 47, p. 7597). During the 1960s a number of factors motivated the R.C.M.P. to push for co-operation by the D.N.R. to fight organized crime. Those factors were: the collapse of certain financial institutions and the involvement of organized crime in associated bankruptcy frauds, a subject which was raised in Parliament and at a 1967 Federal-Provincial Conference; the 1964 Royal Commission on Banking, which mentioned problems in the securities industry; the success of a U.S. task force approach in this field; and the fact that some attorneys general at the 1965 Conference of attorneys general had felt that there should be some co-operation between departments to pursue the income of organized crime

figures (Vol. 47, pp. 7621-27, 7633-34; Vol. 62, pp. 9988-89; Ex. G-1, Tab 12; Ex. G-11, Tab 8; Ex. G-2 for identification, Tab 3).

7. Motivated by these factors, the R.C.M.P. initiated discussions with the D.N.R. with a view to working out arrangements not simply to transmit information to the D.N.R. but also to receive it. One of their reasons for wanting such an exchange was to be able to advise their sources of information that information supplied to the D.N.R. had been put to use. The R.C.M.P. felt that otherwise the sources of information might dry up (Vol. 47, pp. 7667-8).

8. To pursue the objective of closer co-operation, the R.C.M.P. arranged a meeting on November 1, 1967, with D.N.R. officials. According to a record of the meeting the D.N.R. officials present advised the R.C.M.P. that there would have to be a clear understanding in the D.N.R. that the department's involvement was not intended specifically to produce revenue from delinquent taxes but rather to assist in attacking organized crime. The records also show that the D.N.R. officials indicated that the Department did not have the manpower to help the R.C.M.P., but they spoke of the desirability of there being a "two-way exchange", since the then current interpretation of the Income Tax Act "allowed the release of certain information to the police under proper circumstances" (Vol. 62, p. 9988 and Ex. G-1, Tab 11).

9. The next recorded step in the development of this aspect of the relationship is a letter of January 31, 1969, from the Deputy Commissioner (Criminal Ops.) of the R.C.M.P. to the Deputy Minister of National Revenue (Taxation) requesting a meeting to discuss matters which might be of "mutual interest". The letter stated that the purpose of any co-operation would be to combat organized crime, the D.N.R. to assist "through active participation in such investigations". The letter added that the "exchange of information between them" should be a two-way effort (Ex. G-1, Tab 12). Following that letter, a meeting was held on February 18, 1969, between the Deputy Minister of National Revenue (Taxation), the official in charge of special investigations for the D.N.R., Deputy Commissioner Kelly and Assistant Commissioner Carrière, to discuss joint action to combat organized crime. A record of that meeting shows that:

> Kelly stated that this Force would be willing to liaise with members of [D.N.R.] to ensure a two-way exchange of information and where necessary, to treat any information received as strictly confidential. He added that the Force and himself were well aware in view of the content of Section 133 of the Income Tax Act that such a request could not be acceded to as this was not a matter of policy but a matter of law.
>
> (Vol. 47, pp. 7638-42; Ex. G-2 for identification, Tab 4.)

10. Another meeting was held between officials of the D.N.R. and members of the R.C.M.P. on April 23, 1969. The D.N.R. officials advised that Department policy with respect to dissemination of information from their files to the R.C.M.P. was limited to cases where the provisions of section 133(3) of the Income Tax Act applied. Both parties to the meeting admitted that, in spite of the official D.N.R. policy, there were "sometimes *sub rosa* arrangements made

at the Regional Level with respect to specific instances" (Ex. G-1, Tab 13). Prior to 1972 the official policy of both the D.N.R. and the R.C.M.P. was that all requests to the D.N.R. from the R.C.M.P. for assistance were to be directed to R.C.M.P. Headquarters in Ottawa (Vol. 62, pp. 9984-5; Ex. G-2 for identification, Tab 2; Ex. G-1, Tab 14).

11. In his testimony before us, the senior D.N.R. official present at that April 23, 1969 meeting told us that he did not consider that the words in the minutes of the meeting referring to "*sub rosa* arrangements" implied any deviation from official Department policy. He said that he interpreted those words to mean that there would have to be some exchange of information at the district level to determine whether the information was of any value (Vol. 62, pp. 10001-2). He also told us that it was his view at the time of the meeting, that the D.N.R. could furnish information to the R.C.M.P. where the Force would, in some way, assist the Department in collecting tax because that would be an enforcement of the Income Tax Act (Vol. 62, p. 9998). It is clear from the evidence before us that the official position of the D.N.R. at that time was that information could only be communicated to another agency if to do so would assist the Department in administering or enforcing the Income Tax Act (Vol. 47, p. 7651; Ex. G-1, Tab 14).

12. We have noted that on September 15, 1969, the officer in charge of the R.C.M.P. Legal Branch gave a legal opinion to the assistant officer in charge of the C.I.B. which stated that, before information could legally be given to the R.C.M.P. by the D.N.R. under section 133, "there must be a tax interest" (Ex. G-1, Tab 15).

13. Another high level meeting was held on October 29, 1969, between the Deputy Minister and officials of the D.N.R., and R.C.M.P. officers, to discuss a draft memorandum which had been prepared by the two agencies on the subject of "Co-operation relative to the investigation of organized crime". At that meeting the Deputy Minister insisted that there had to be a tax interest before any tax information could be released by an authorized person. The record of the meeting shows that the R.C.M.P. representatives present agreed with that interpretation and agreed to the deletion from the draft memorandum of a statement to the contrary which said, in referring to section 133(7)(a) of the Income Tax Act:

> These words could also be construed to mean that an authorized person could release the required information as part of his day-to-day job, and that no particular tax interest is necessary.

The Deputy Minister also advised the R.C.M.P., at that meeting, that direction would have to be sought from the government for the change in policy by the D.N.R. which would result from this new area of co-operation. He suggested that the R.C.M.P. prepare a draft memorandum to Cabinet for the signature of the Solicitor General (Vol. 47, pp. 7704-5; Ex. G-2 for identification, Tab 5).

14. At some point, probably in 1969, the Commissioner of the R.C.M.P. asked the Honourable G.J. McIlraith, the Solicitor General, to do something to enable the R.C.M.P. to obtain direct access to income tax returns for the

purpose of dealing with the subject of organized crime. In a letter dated January 21, 1970 to Mr. McIlraith, Commissioner Higgitt discussed obtaining access to tax data to attack organized crime from the revenue viewpoint. Mr. McIlraith testified that during that same period he had discussions with Commissioner Higgitt about the R.C.M.P.'s desire to get information from the D.N.R. to assist in the investigation of certain criminals in the organized crime field (Vol. 120, pp. 18707-9).

15. On March 20, 1970, the R.C.M.P. forwarded to Mr. McIlraith a copy of a draft memorandum to Cabinet which had been prepared by the D.N.R. and the R.C.M.P. (Vol. 47, p. 7705; Ex. G-2 for identification, Tabs 7 and 8). Mr. McIlraith told us that he was supportive of the R.C.M.P. obtaining clarification of what they were entitled to get from the D.N.R. He also told us that, from the time he was first approached with a request to do something to obtain direct access by the R.C.M.P. to income tax returns until he left the Solicitor General's portfolio on December 22, 1970, he refused to do anything about that aspect (Vol. 118, pp. 18472-4; Vol. 120, pp. 18707, 18734).

16. Following the receipt by Mr. McIlraith of the draft memorandum to Cabinet, which was forwarded to him on March 20, 1970, Commissioner Higgitt noted in his diary on April 23, 1970:

> Solicitor General asked re cooperative action by Income Tax Branch and R.C.M.P. Solicitor General said he would suggest to the Minister of National Revenue that the Act gave sufficient leeway.
>
> (Vol. 120, p. 18718; Ex. M-75.)

Several months later Commissioner Higgitt recorded in his diary entry of September 8, 1970 that he had had a meeting with Mr. McIlraith and he noted the following:

> Jogged Solicitor General's memory re income tax cooperation. He said he had spoken to the Minister (Mr. Côté) last week. He said his departmental people thought there ought to be a Cabinet paper. He, Côté, did not agree and would like the Solicitor General to clarify the matter before him, etc. This is to be done as soon as convenient.
>
> (Vol. 120, pp. 18722, 18733-34, Ex. M-76.)

On December 22, 1970, the Honourable Jean-Pierre Goyer succeeded Mr. McIlraith as Solicitor General. Sixteen months later, a joint memorandum to Cabinet dated April 27, 1972, signed by Mr. Goyer and the Minister of National Revenue, sought approval for the D.N.R., with the assistance of the R.C.M.P., to

> . . . conduct a continuing programme of tax investigations into the affairs of members of Organized Crime with a view to their prosecution under the Income Tax Act on the clear understanding that the restrictions set forth in section 241 of the Income Tax Act apply to members of the Force engaged in this enterprise and that they will be instructed not to communicate or knowingly allow to be communicated to any person other than to those persons designated by the Minister of National Revenue any information obtained by or on behalf of the Minister of National Revenue for the purposes of that Act.

The memorandum also provided: "No public announcement is contemplated" (Vol. 123, p. 19202; Ex. G-2c, Tab 7). The Cabinet granted approval for this programme, which was known as the Tax Programme, on May 25, 1972. Mr. Goyer testified before us that the objective of this contemplated programme was to combat organized crime while administering the Income Tax Act (Vol. 123, p. 19202).

17. Also on April 27, 1972, a Memorandum of Understanding between the Department of National Revenue (Taxation) and the Department of the Solicitor General was prepared and signed by the Deputy Ministers of the two Departments. This memorandum was subject to the approval by Cabinet of the proposal contained in the memorandum to Cabinet. In this Memorandum of Understanding, the method of putting into operation the proposal contained in the memorandum to Cabinet was made more specific. It provided as follows:

1. The Minister of National Revenue, pursuant to the provisions of subsection (4) of Section 241 of the Income Tax Act, hereby designates the members of the Directorate of Criminal Investigations of the Royal Canadian Mounted Police as authorized persons for the purpose of assisting him and his officials in carrying out investigations for such purposes as the Minister of National Revenue may designate related to the administration or enforcement of the Income Tax Act.
2. The Royal Canadian Mounted Police acknowledges that the members of the Directorate of Criminal Investigations of the Royal Canadian Mounted Police will conduct for the purposes of the Income Tax Act, such investigations of such persons as the Minister of National Revenue may from time to time request, except when the Solicitor General is of the opinion that having regard to the current tasks of the Royal Canadian Mounted Police and the availability of manpower, it is not practical for such investigations to be conducted.
3. The Minister of National Revenue will furnish the Directorate of Criminal Investigations of the Royal Canadian Mounted Police with such information or material in his possession which in the Minister's opinion will facilitate the conduct of any investigation which the Directorate of Criminal Investigations of the Royal Canadian Mounted Police is carrying out on behalf of the Minister.
4. The Royal Canadian Mounted Police acknowledges that all information obtained for the purposes of the Income Tax Act by the members of the Directorate of Criminal Investigations of the Royal Canadian Mounted Police in the conduct of investigations referred to in clause 2 hereof are subject to the restrictions set forth in Section 241 and that in particular, no member of the Directorate of Criminal Investigations of the Royal Canadian Mounted Police will knowingly communicate or knowingly allow to be communicated to any person other than those persons designated by the Minister of National Revenue any information obtained by or on behalf of the Minister of National Revenue for the purposes of this Act.
5. The Solicitor General of Canada agrees to provide the Minister with the names of individuals whom the Directorate of Criminal Investigations of the Royal Candian Mounted Police suspects of being involved in organized crime and in evading or understating the amount of their income,

together with all intelligence information available to it on these individuals.

6. The Minister acknowledges that all information which he receives from the Solicitor General of Canada either prior to or as a result of investigations which have been carried on by members of the Directorate of Criminal Investigations of the Royal Canadian Mounted Police as authorized persons will be treated as confidential information and will not, without the express authority of the Royal Canadian Mounted Police, be disclosed to persons other then [sic] designated individuals who are members of the Special Investigations Division of the Department of National Revenue and their superior officers.

7. The Minister agrees that if he should conclude that any investigation which is being conducted by members of the Directorate of Criminal Investigations of the Royal Canadian Mounted Police pursuant to the provisions of clause 2 hereof is not likely to be fruitful and is being discontinued by his officials, he will immediately so advise the Directorate of Criminal Investigations of the Royal Canadian Mounted Police.

8. Members of the Directorate of Criminal Investigations of the Royal Canadian Mounted Police will assist National Revenue, Taxation to develop evidentiary standards to establish offences on the basis of testimony relative to cash transactions where documentation is limited or non-existent and will, in circumstances considered appropriate by both National Revenue, Taxation and the Royal Canadian Mounted Police, allow its criminal intelligence investigators to give evidence in court on their knowledge of financial transactions entered into and business procedures and techniques used by members of organized crime prosecuted by National Revenue, Taxation.

9. This agreement will take effect upon the approval by Cabinet of the recommendations contained in a memorandum to Cabinet by the Minister of National Revenue and concurred in by the Solicitor General dated April 27, 1972.

18. The Department of Justice assisted with the content and the drafting of the Memorandum of Understanding and gave an opinion that the agreement was legal. The Attorney General of Canada approved of the memorandum to Cabinet when it was drafted (Vol. 62, pp. 10011-16; Vol. C12, p. 1327).

19. According to the testimony before us of Inspector R.D. Crerar, the officer in charge of the R.C.M.P. Commercial Crime Branch, the kind of exchange of information envisaged by the Memorandum of Understanding is not different from that which was discussed at the meeting of April 23, 1969, i.e. it was limited to cases where the provisions of section 133(3) of the Income Tax Act applied (Vol. 47, pp. 7646-47).

20. It will be noted that the Memorandum of Understanding designated the members of the Directorate of Criminal Investigations as "authorized persons". Testimony before us disclosed that the Directorate of Criminal Investigations included the Commercial Crime Branch (C.C.B.), the National Crime Intelligence Branch (N.C.I.B.), the Contract Policing Branch, the Native Policing Branch, the Customs and Excise Branch, the Federal Policing Branch, the Drug Enforcement Branch and the Special "I" Branch. However, com-

munications from R.C.M.P. Headquarters to the divisions limited the application of the programme to the Commercial Crime Branch and the National Crime Intelligence Branch. The evidence also disclosed that within the R.C.M.P., the primary responsibility for carrying out the Tax Programme was assigned to the C.C.B. and the N.C.I.B., although there were times when other members were involved (Vol. 48, pp. 7741-45; Vol. C12, p. 1432).

21. We were told that it was the understanding of the D.N.R. that certain R.C.M.P. members within the Directorate of Criminal Investigations would be assigned to the Tax Programme and that they would be the "designated" persons. The R.C.M.P. did assign certain members to the programme (Vol. 62, p. 10019; Vol. 48, pp. 7753-55, Ex. G-1, Tab 17). The D.N.R. were assured by the R.C.M.P. that the Force would not disseminate taxation data outside the Force, and would only disseminate it within the Force on a strict 'need to know' basis. We heard evidence, which we shall discuss later in this chapter, that tax information was given to members of the R.C.M.P. who were not on the Tax Programme provided they had a 'need to know' (Ex. G-1, Tab 17, Vol. 48, pp. 7758-60). The current arrangement is that all R.C.M.P. members designated under the Tax Programme must be designated in writing by the Director of Criminal Investigations (Vol. 48, pp. 7830-39; Ex. G-1, Tab 23).

22. There was considerable evidence as to who were included in the definition of "organized crime" but, as we mentioned earlier, because we do not consider that a definition of that phrase affects the legal issues involved, we do not propose to summarize the evidence nor to come to any conclusion about it. It is clear that the D.N.R. did not particularly concern itself about a definition of "organized crime". An official of the D.N.R. involved in the Tax Programme testified that the Department always understood that the people being investigated under the programme were those involved in criminal activities and that the term "organized crime" was a more common phrase used to describe them (Vol. 62, pp. 10030-31; Ex. G-12, Tab 11B). As Mr. Justice Laycraft observed in 1978 the working definition of "organized crime" used by the R.C.M.P. is so wide as to include any two persons committing a second offence, and even "any person making his living from crime".[1]

23. Regardless of who is included in the definition of "organized crime", there does not appear to have been any difficulty or disagreement as to who ought to be the subjects or "targets" of the programme. Initially, the targets of the programme were provided by R.C.M.P. Headquarters. Subsequently, targets were selected at the local district level by agreement between the D.N.R. district official and the R.C.M.P. Unit or Section Commander. The R.C.M.P. Unit advised R.C.M.P. Headquarters of each such selected target, and on no occasion did Headquarters veto such a selection. The evidence disclosed that both the R.C.M.P. and the D.N.R. could suggest names of potential targets for consideration (Vol. 62, p. 10135; Vol. 62, p. 10058; Ex. G-11, Tab K; Vol. C48, p. 7767-72, and Ex. G-2, Tab 11).

---

[1] *Report of a Public Inquiry into Royal American Shows Inc. and its Activities in Alberta*, June 1978, at p. C-42.

24. The memorandum to Cabinet seeking approval for the Tax Programme indicated that no public announcement of the programme was contemplated, but there is nothing in the Memorandum of Understanding nor in the Cabinet decision that prohibits publication of the agreement. There was, however, an agreement between the Department of National Revenue and the Solicitor General's Department that the Memorandum of Understanding would not be published. Later, some pressure developed within the government to disclose publicly the existence of the Tax Programme. By letter dated March 11, 1975, the Honourable Ronald Basford, the Minister of National Revenue, wrote to the Solicitor General, the Honourable Warren Allmand, advising that it was his intention to make a public announcement regarding the programme. It appears that Mr. Allmand sought the advice of Commissioner Nadon on the matter, because a letter dated April 7, 1975, from Commissioner Nadon to Mr. Allmand, set out the arguments on both sides with respect to publication. That letter discloses that the main reason why, according to the R.C.M.P., the agreement should not be made public was that pressure groups would seek an amendment to the Income Tax Act which would make the Act more restrictive. Commissioner Nadon told us that, on balance, he had favoured publication of the agreement.

25. Mr. Allmand concluded that it was necessary to make a public announcement and, by letter dated May 10, 1976, he wrote to the Honourable Bud Cullen, the Minister of National Revenue, stating that it was imperative that some form of public announcement be made by Mr. Cullen's office. Mr. Cullen replied, by letter dated June 9, 1976, agreeing that there ought to be an announcement but added that there were some problems to be considered. He told Mr. Allmand that Cabinet authority for the agreement had been obtained on the assurance that no public announcement would be made and therefore express authority would have to be sought from Cabinet for a public announcement. He suggested that Mr. Allmand take the initiative in seeking such Cabinet approval and that he would support Mr. Allmand's position.

26. It is clear from the evidence that the R.C.M.P. and the D.N.R. had different reasons for wanting to keep the agreement secret. The R.C.M.P. wanted to keep it secret in order to combat organized crime. However, as time passed the targets of the programme became aware that they were being investigated by the R.C.M.P. through the reporting of cases coming before the courts in which the R.C.M.P. had acted as witnesses. As more targets became aware of the investigations there was less reason for the R.C.M.P. to maintain the confidentiality of the agreement. The reason the D.N.R. wished to keep the agreement secret was their concern that publication of it would damage the credibility of their assertion of the confidentiality of tax information.

27. Publication of the agreement eventually took place in the Fall of 1977, when its existence was made public as a result of the Inquiry of Mr. Justice Laycraft in Alberta.[2] Commissionner Nadon testified at the Laycraft Inquiry without the benefit of a review of the R.C.M.P. documentation with respect to possible publication of the agreement. He testified at that Inquiry that from

---

[2] *Ibid.*

the outset, and during the course of the agreement, the R.C.M.P. had endeavoured to have it published, whereas the evidence before us disclosed that at least on one occasion the R.C.M.P. were satisfied that publication would not be desirable.

28. On March 3, 1977, Commissioner Nadon met with the Attorney General of Alberta and at the meeting admitted that there was an agreement with the D.N.R., but he advised the Attorney General that its contents were confidential. Mr. Nadon refused to let the Attorney General see a copy of the agreement unless the D.N.R. first agreed to such disclosure. He advised the Attorney General that when the agreement was first entered into the R.C.M.P. had been in favour of it being published but that the D.N.R. had been opposed. Mr. Nadon told us that he considered that the agreement between the two departments not to publish superseded his responsibility in his relationship with the Provincial Attorney General because any disclosure by the R.C.M.P. would not only jeopardize other arrangements they had with the D.N.R. but also might preclude further information from being provided to the Force. (We discuss the relationship between the R.C.M.P. and provincial attorneys general in Part X, Chapter 4.)

Extent and prevalence

29. At our request, a memorandum dated December 20, 1977, was sent from R.C.M.P. Headquarters to the commanding officers of all R.C.M.P. divisions asking, *inter alia*, for the following information:

> Between 1969 and 1972, did R.C.M.P. Investigators obtain information from Income Tax files in contravention of Section 241 of the Income Tax Act? If so, under what circumstances, how many times etc.?
>
> *Subsequent to the 1972 Agreement*
>
> Were there any incidents when information received as per the Agreement was used for purposes other than enforcement of the Income Tax Act? e.g. disclosed to other R.C.M.P. sections which did not have lawful access such as — Security Service, Criminal Investigative Sections. If so, how many times, under what circumstances?

30. For the period from 1969 to 1972, the replies to that request for information did not disclose any specific cases of dissemination of information in contravention of the Income Tax Act. The reasons given in those replies are either that no such information was provided to the R.C.M.P. or that no records are available for that period to enable a reply to be given. The evidence discloses that there was, however, a recollection that the D.N.R. sometimes supplied biographical information to the Force (Ex. G2C, Tabs 12-27 inclusive, Vol. 48, pp. 7861-7910).

31. The replies, which were filed as exhibits with us, disclose that, for the period following the 1972 Memorandum of Understanding to the respective dates of reply from the divisions, there were numerous instances in which information was sought by R.C.M.P. members assigned to the Tax Programme and passed on by them to other branches of the R.C.M.P. and to other police forces, when such information was not being used for the purpose of enforce-

ment of the Income Tax Act. The evidence shows that in most of those cases the information was of a biographical nature but that in some cases it included financial information (Ex. G2C, Tabs 12-27; Vol. 48, pp. 7861-7910; Vol. 50, pp. 8016-43; Vol. 51, pp. 8260, 8270, 8317; Vol. 63, pp. 10320-32). The evidence also discloses that in many instances the D.N.R. officials involved were aware that the information they were passing to the R.C.M.P. members was not for the purposes of enforcement of the Income Tax Act (Ex. G-11, Tabs 1-28).

32. We were also told in testimony that there have been instances where the R.C.M.P. members involved in the Tax Programme have come across evidence of serious criminal offences and have felt that they were not able to proceed to prosecution with respect to those offences because they were not entitled to use the information for that purpose (Vol. 48, pp. 7850-6; Vol. 49, pp. 7945-6).

Legal issues

33. The Income Tax Act,[3] section 241, provides for the confidentiality of information given by a taxpayer to the Department of National Revenue. It also sets forth exceptions. It also makes it an offence to contravene the section. The relevant parts of the section are as follows:

> 241. (1) Except as authorized by this section, no official or authorized person shall
>
> (a) knowingly communicate or knowingly allow to be communicated to any person any information obtained by or on behalf of the Minister for the purposes of this Act, or
>
> (b) knowingly allow any person to inspect or to have access to any book, record, writing, return or other document obtained by or on behalf of the Minister for the purposes of this Act.
>
> (2) Notwithstanding any other Act or law, no official or authorized person shall be required, in connection with any legal proceedings,
>
> (a) to give evidence relating to any information obtained by or on behalf of the Minister for the purposes of this Act, or
>
> (b) to produce any book, record, writing, return or other document obtained by or on behalf of the Minister for the purposes of this Act.
>
> (3) Subsections (1) and (2) do not apply in respect of criminal proceedings, either by indictment or on summary conviction, under an Act of the Parliament of Canada, or in respect of proceedings relating to the administration or enforcement of this Act.
>
> (4) An official or authorized person may,
>
> (a) in the course of his duties in connection with the administration or enforcement of this Act,
>
> (i) communicate or allow to be communicated to an official or authorized person information obtained by or on behalf of the Minister for the purposes of this Act, and

[3] R.S.C. 1970, ch.I-5, as amended by S.C. 1978-79, ch.5.

(ii) allow an official or authorized person to inspect or to have access to any book, record, writing, return or other document obtained by or on behalf of the Minister for the purposes of this Act;

(b) under prescribed conditions, communicate or allow to be communicated information obtained under this Act, or allow inspection of or access to any written statement furnished under this Act to the government of any province in respect of which information and written statements obtained by the government of the province, for the purpose of a law of the province that imposes a tax similar to the tax imposed under this Act, is communicated or furnished on a reciprocal basis to the Minister;

(c) communicate or allow to be communicated information obtained under this Act, or allow inspection of or access to any book, record, writing, return or other document obtained by or on behalf of the Minister for the purposes of this Act, to or by any person otherwise legally entitled thereto; or

(d) communicate or allow to be communicated to a taxpayer, such information obtained under this Act regarding the income of his spouse or of any other person as is necessary for the purposes of an assessment or reassessment of tax, interest, penalty or other amount payable by the taxpayer or of the determination of any refund to which he is entitled for the year.

(a) *The general rule stated in section 241 of the Income Tax Act*

34. The section attempts to protect from unauthorized disclosure, a term which is discussed below, "any information obtained by or on behalf of the Minister for the purposes of this Act". It further restricts inspection of or access to "any book, record, writing, return or other document obtained by or on behalf of the Minister for the purposes of this Act."

(b) *The exceptions*

35. There are a number of exceptions to the general rule prohibiting disclosure. The rule does not apply in respect of criminal proceedings, either by indictment or on summary conviction, under an Act of the Parliament of Canada, or in respect of proceedings relating to the administration or enforcement of the Income Tax Act. Furthermore, an "official" or "authorized person" may:

(i) in the course of his duties in connection with the administration or enforcement of the Act, communicate or allow to be communicated to an official or authorized person tax information and allow an official or authorized person to inspect documents obtained for the purposes of the Act;

(ii) communicate information or allow inspection of documents to or by the government of any province for the purpose of administering a tax law of the province;

(iii) communicate information or allow inspection of documents to any person "otherwise legally entitled thereto";

(iv) communicate information to a taxpayer regarding the income of his spouse or of any other person in order to permit an assessment or reassessment of tax, interest, penalty, etc.

In addition, the Minister may permit a copy of a document containing tax information to be given to the person from whom such document was obtained, or to that person's legal representative or agent.

36. Who is an "official or authorized person" for the purposes of section 241 of the Income Tax Act? Section 241(10)(a) defines "official" as

> . . . any person employed in or occupying a position of responsibility in the service of Her Majesty, or any person formerly so employed or formerly occupying a position therein;

Subsection (b) of section 241(10) defines "authorized person" as

> . . . any person engaged or employed, or formerly engaged or employed, by or on behalf of Her Majesty to assist in carrying out the purposes and provisions of this Act;

37. The major difference between "official" and "authorized person" is that the section does not specify that the job or function of an "official" necessarily requires that it be "to assist in carrying out the purposes and provisions of this Act." It thus appears that an R.C.M.P. officer could fall within the definition of "official" as being "employed in or occupying a position of responsibility in the service of Her Majesty". This was the view of Mr. Justice Laycraft, in the Alberta inquiry.[4] If this is the case, then an R.C.M.P. officer does not need to be designated by anyone as an authorized person, and the prohibitions and sanctions of section 241 apply automatically as long as he is dealing with what has been termed above, for the sake of brevity, as tax information, and as long as this information has been "obtained by or on behalf of the Minister for the purposes of this Act."

38. On the other hand, an R.C.M.P. officer may become an "authorized person" if he is either seconded to the Department of National Revenue, or hired by the Department to perform work in connection with the Act or in some way "engaged. . . to assist in carrying out the purposes and provisions" of the Income Tax Act. Then he automatically becomes an "authorized person" and does not need to be so designated by anyone. The question whether someone is an "official" or "authorized person" thus becomes a question of fact.

39. What restrictions apply to the dissemination of biographical data provided to the Department of National Revenue by a taxpayer? Not only does section 241 of the Income Tax Act protect "any information obtained" as long as it is obtained for "the purposes of" the Act; it restricts access to any "book, record, writing, return or other document obtained" . . ."for the purpose of this Act."

---

[4] *Report of a Public Inquiry into Royal American Shows Inc. and its Activities in Alberta*, June 1978, pp. C-42-47.

40. One of the qualifying phrases is "for the purposes of this Act". The question then arises whether biographical information is information obtained for the purposes of the Act. Biographical information, as distinguished from financial information, would include the taxpayer's name, address, telephone number, employer's name, wife's and children's names, previous addresses, S.I.N. number and any other information describing the identity or personal situation and history of the taxpayer. It may be argued that this information is necessary in order that the Department of National Revenue be able to make a positive identification of the taxpayer and in at least that sense it is information obtained "for the purposes of the Act." Indeed, that was the conclusion reached by the Ontario Court of Appeal in a recent case, *Glover* v. *Glover*[5] The reasons for decision in that case said:

> The address of the taxpayer is a necessary and integral part of the information sought and received for the purposes of the Income Tax Act. To deliberately misstate the address is an offence under the Act. The section does not allow the Court to weigh the quality or relative value of the information. It prohibits the communication of "*any*" information received for the purposes of the *Income Tax Act*. In my opinion, the address received by the Minister of taxpayers on the Income Tax returns is information obtained by or on behalf of the Minister for the purposes of the *Income Tax Act*. Such information can only be communicated to persons authorized to receive it by virtue of the exceptions or qualifications contained in s.241.

41. We accept that analysis and proceed on the basis that it is correct. May an "official" or "authorized person" use information covered by section 241 to pursue an investigation or proceed with the prosecution of an offence unrelated to the Income Tax Act? Before the 1966 Amendments, which resulted in the current section 241, various court decisions held that in certain circumstances tax information could be used in a court of law, since the prohibition applied only to administrative and not to judicial proceedings. A judge sitting in a court of law was seen to be a person legally entitled to the information within the meaning of the section of the Act. The 1966 amendments indicate that no official or authorized person shall be required, in connection with any legal proceedings, to communicate or to give evidence of any tax information or produce tax records obtained for the purpose of the Act, unless such communication or testimony is in respect of criminal proceedings under a Federal statute, or in respect of proceedings relating to the administration or enforcement of the Income Tax Act (Section 241(3)). Despite the exclusion in subsection 3, of a reference to other civil proceedings, subsection 4(c) indicates that:

> (4) An official or authorized person may... (c) communicate...[tax] information... or allow inspection of or access to any book, or other [tax] document...*to or by any person otherwise legally entitled thereto.*
>
> (Emphasis is ours.)

In *Glover* v. *Glover*[6] it has now been held that a court is not a "person otherwise legally entitled thereto".

---

[5] *Glover* v. *Glover*, [1980] D.T.C. 6262 (Ont. C.A.).

[6] *Ibid.*

42. However, apart from the question of whether a court is entitled to have such information, there has as yet been no judicial interpretation of the section as to whether a member of the R.C.M.P. who is given the information for purposes, as far as the Revenue official is concerned, of the administration of the Income Tax Act, may use the information in *his own* investigation of an offence unrelated to the Act. We think the Act does not prohibit such a use. However, if he communicates the information to another member of the R.C.M.P. or a member of another police force, we do not think that he may lawfully do so, for he is then not making the disclosure for the purpose of the Act. If, as was held in *Glover* v. *Glover*, the court is not entitled, we cannot see that a policeman conducting a criminal investigation unrelated to the Act is entitled.[7] In Part X, Chapter 5, we shall recommend changes in the law so that the R.C.M.P. would have access to tax information to investigate offences unrelated to the Income Tax Act. Such access should be governed by a system involving judicial authorization, similar to that which now exists for the use of electronic surveillance. Whether the R.C.M.P. should be able to distribute tax information received under judicial authorization to other police forces is a matter for the Solicitor General of Canada to discuss with the provincial attorneys general.

43. Our conclusions are that:

(a) Furnishing of information, given to the Department by the taxpayer on his income tax return, to the R.C.M.P. for purposes other than enforcement of the Income Tax Act — for example, for a criminal investigation — is and has been a contravention of the Act on the part of any Departmental official communicating the information. If, in any of the specific cases, a member of the R.C.M.P. abetted (encouraged) the source, he was a party to the offence under section 21 of the Criminal Code. If he "counselled" or "procured" the source to commit it, he was a party to the offence under section 22 of the Criminal Code. We did not receive evidence as to such encouragement, counselling or procurement in specific cases. We note that the offence is a summary conviction offence; therefore there cannot be prosecution except within six months of the offence.

(b) No offence was committed if the information was communicated after the commencement of criminal proceedings.

(c) Furnishing such information to the R.C.M.P. for the purpose of the Income Tax Act, which was the express intention of the Memorandum of Understanding, was not in contravention of the Act.

(d) If any member of the R.C.M.P. who received such information passed it on to another member not engaged in an investigation relating to the enforcement of the Act, he may have committed an offence.

---

[7] This subject was also discussed by Mr. Justice Laycraft in his *Report of a Public Inquiry into Royal American Shows Inc. and its Activities in Alberta*, June 1978, at p. C-45.

C. UNEMPLOYMENT INSURANCE COMMISSION

44. Canadians are required by statute to provide information about themselves to the Unemployment Insurance Commission, both at the time of registering for a Social Insurance Number, and when applying for benefits. The Criminal Investigation Branch has been seeking access to this information to help to locate persons wanted for the commission of crime, to identify bodies and stolen property, and to find missing persons. In this section we give an account of the history, over 30 years, of the C.I.B.'s involvement with the U.I.C., and combine it with a discussion of the legal issues, for during that period there were several changes in the statute or in regulations, and it is therefore clearer and more convenient to mix fact and law.

1946 to 1965

45. There were no confidentiality provisions in the applicable statutes before 1946[8] and the transfer of information from the Unemployment Insurance Commission to the R.C.M.P. before that year raised no legal issues other than those that arise whenever a federal government employee gives official information to the police. In 1946 a confidentiality provision, section 105, was written into the Unemployment Insurance Act. It provided that

> Information, written or verbal, obtained by the Commission from any person pursuant to the provisions of this Act or any regulations made thereunder shall be made available only to the employees of the Commission in the course of their employment and such other persons as the Commission may deem advisable...[9]

Non-compliance with a requirement of the Act was made an offence in the same amendments and this has been a feature of the unemployment insurance legislation ever since. Therefore the release of confidential information to the R.C.M.P. was an offence unless the release complied with the requirement of section 105 that the Commission deem it advisable. It is clear from the evidence before us that members of the R.C.M.P. actively participated with personnel of the U.I.C. in obtaining confidential information after 1946, and therefore may have committed an offence of conspiracy to effect an unlawful purpose, contrary to section 423(2)(b) of the Criminal Code, or of abetting a person to commit an offence, contrary to section 21(1)(c) of the Code.

46. However, before it can be asserted that offences had in fact been committed, the following questions must be answered:

(a) Was it necessary that the discretion conferred by the confidentiality provision be exercised by the Unemployment Insurance Commission itself?

(b) If so, could the Commission delegate this discretion, and can it be proved to have done so?

(c) Could the discretion be exercised by an employee of the Commission, without authority to do so having been delegated by the Commission?

---

[8] See the Unemployment Insurance Act, 1940, S.C. 1939-40, ch.44.

[9] 1946 S.C., ch.68.

47. The first record of R.C.M.P. policy on the matter dates from December 1950, when members of the Force were permitted to seek information from the U.I.C. at its regional offices about individuals "who are being sought on criminal grounds and also respecting missing persons" (Vol. 57, pp. 9354-5). This policy was based on a letter dated December 9, 1950, from the Executive Director of the U.I.C. to the R.C.M.P. (Vol. 57, pp. 9352-3). A senior officer of the R.C.M.P. advised the officer in charge of the C.I.B. and the officer in charge of the Identification Branch that it would be "well to refer to the Commission only those cases where other enquiries are not productive" (Ex. H-1, p. 12). The policy became part of the R.C.M.P. Policy Manual in about 1964. In the same year the Social Insurance Number (S.I.N.) system was introduced by regulation[10] under both the Unemployment Insurance Act and the Canada Pension Plan Act. On June 4, 1964, the Ontario Division advised the U.I.C. that they would seek "information on the holder of a U.I.C. number and/or a new Social Insurance Number" (Ex. H-1, p. 15). Yet at or about this time the question was raised in the House of Commons as to whether information on a social registration card would be be made available to the R.C.M.P. On June 5, 1964 the then Commissioner of the R.C.M.P. wrote to the Minister of Justice, advising him that the Force was not using the information from the social security registration system and had no intention of seeking access to it (Vol. 57, pp. 9367-73).

48. On June 11, 1964, a Deputy Commissioner wrote to the Commanding Officers of all R.C.M.P. divisions advising them that the Commissioner of the R.C.M.P. had assured the Minister of Justice that the Force had no intention of seeking access to the information compiled during the social security registration programme and that "In line with this policy, no attempts are to be made by any member of the Force to obtain access to this material". Copies of this letter were sent to the Director of Security and Intelligence and the Director of Criminal Investigations (Ex. H-1, p. 16; Vol. 57, p. 9378). Two weeks later, however, the same Deputy Commissioner wrote a further memorandum to the Commanding Officers of all divisions (Ex. H-1, p. 17) which stated that access to the U.I.C. records was to continue whether the information had been given to the U.I.C. under the old alphabetical prefix system or the new number prefix system (Vol. 57, pp. 9392-3).

1965 to 1971

49. In 1965 the Canada Pension Act[11] was enacted. Sections 100 to 106 of this statute required that persons in "pensionable employment" file an application with "the Minister" for a Social Insurance Number. This provision cast a far larger net than the Unemployment Insurance Commission Act since it also covered self-employed persons. Section 107 of this statute contains the confidentiality provisions. These provisions differed considerably from the confidentiality section of the Unemployment Insurance Commission Act. Section 107 restricted the release of S.I.N. information compiled under that Act and would

[10] See P.C. 1964-379; (S.O.R./64-108).
[11] S.C. 1964-1965, ch.51.

prohibit the release of information to the R.C.M.P. for the purpose of law enforcement at large.

50. The C.P.P. (S.I.N.) Regulations[12] were enacted on August 11, 1965. These Regulations provided that a person required to apply to the Minister for a S.I.N. under the Canada Pension Plan Act was to do so by delivering or mailing his or her application to the local office of the U.I.C. (section 3(1)).

51. The evidence discloses that the S.I.N. information obtained by the U.I.C. under the provisions of the Canada Pension Plan Act was compiled in the Central Index of the U.I.C. The evidence shows also that the U.I.C. made no attempt to segregate Unemployment Insurance Commission Act information and Canada Pension Plan Act information in its Central Index, and responded to all requests by the R.C.M.P. for S.I.N. information.

52. While there is some evidence that the Force, including the Commissioner and Deputy Commissioner, were aware of the two different sources of S.I.N. information, there is no evidence that the Force was aware of the different confidentiality provisions in the two statutes. However, the evidence shows that the Force sought no legal opinion concerning these issues at any time during this period. According to the testimony of Assistant Commissioner Jensen, he always considered the matter to be an administrative, rather than a legal, concern. It is not unfair to interpret this view to mean that, as long as an employee of the U.I.C. in an apparent position of responsibility was prepared to release information, the R.C.M.P. would use it for the purpose of law enforcement generally.

53. In new instructions to members of the Force in 1967 reference was made for the first time to the Central Index of the U.I.C. It stated that requests for record checks could be made by divisions, branches, etc. to the U.I.C. offices and/or Central Index at Ottawa.

54. In June 1969 the Chief Supervisor of the Central Index of the U.I.C. advised by letter that he had no objection to R.C.M.P. field divisions sending requests for information directly to the Central Index by telex, and the R.C.M.P. Policy Manual was amended accordingly. The amendment advised that any telex message should indicate that the information was "being sought in connection with a criminal offence". It was clear in this policy that Social Insurance Numbers could be used. However, the Minister of Justice was not advised that the Force's position was now different from that which had been stated by the Commissioner to the Minister on June 5, 1964 (Vol. 57, p. 9405).

1971 to 1977

55. From early in 1971 until the fall of 1972 the formal flow of information from the U.I.C.'s Central Index was considerably restricted, to the point that it was all but terminated (Ex. H-1; Vol. 57, pp. 9408-23; Vol. 60, pp. 9827-8). In 1971 the Unemployment Insurance Commission Act was under debate in the House of Commons. It appears from the record that the restriction may have resulted from these debates; it was certainly contemporaneous.

[12] P.C. 1965-1458; (S.O.R./65-372).

56. The Unemployment Insurance Commission Act, 1971, assented to on June 23, 1971, carried forward the confidentiality provision previously found in section 105, in what now became section 114.[13] However, the statute elevated the U.I.C.'s S.I.N. registration system from the status of Regulations to that of a statute (see sections 125 and 126). With this elevation came a new confidentiality section, section 126(4), which provides as follows:

> (4) The Commission may, subject to such regulations as the Governor-in-Council may make in that behalf, make available such information contained in the registers maintained under section 125 or this section as the Commission deems necessary for the accurate identification of individuals and for the effective use by such individuals of Social Insurance Numbers and Social Insurance Number Cards, to such persons as the Commission thinks appropriate to accomplish such purpose.

This confidentiality section, rather than section 114, clearly applies to Central Index information (viz: S.I.N. information).

57. In August of 1972 the R.C.M.P. was made aware of the existence of section 126(4) and in fact was advised that that section in part was the reason for the change in position by U.I.C. personnel (Ex. H-1, p. 37).

58. Up to this time it appears from the record that the R.C.M.P. took the view that the predecessors of section 114 applied and took the further position that the question whether the R.C.M.P. were persons whom the Commission deemed "advisable" was an administrative issue, not a legal one. However, at this point the R.C.M.P. did not seek a legal opinion. Instead it either continued to assume that section 114 applied or was content to rely upon whatever "administrative" decision was made by the employee of the U.I.C. with whom it was dealing at the time.

59. In August and September 1972 the Executive Director of the U.I.C. confirmed that the R.C.M.P.'s operations manual provisions as to access to U.I.C. Central Index information "is acceptable to me but of course this does not constitute the Commission's policy..." (Ex. H-1, p. 42). The R.C.M.P. manual was amended in October 1972, in such a way that members of the Force were aware that information from the Central Index was again available. There is no evidence that the Unemployment Insurance Commission itself ever approved the arrangement (Vol. 57, pp. 9431-4). Enquiries were to be limited to certain specific major crimes "or any other serious crime" (Ex. H-1, p. 41). Assistant Commissioner Jensen told us that the words "serious crime" would mean any indictable offence under the Criminal Code or any federal statute (Vol. 57, pp. 9438-40). R.C.M.P. Headquarters sought information in regard to any type of "crime" until late 1976. At that time, as a member of the R.C.M.P. testified before us, information was to be requested only when it related to a crime on the list found in the 1972 arrangement or any other cases approved by a specific regular member of the Force at Headquarters (Vol. 58, pp. 9564-71). The witness testified that indeed the policy permitted the Force to obtain information for "some other purpose that is considered to be in the public interest": this included Security Service matters, missing persons and

[13] S.C. 1970-71-72, ch.48.

deceased persons (Vol. 58, pp. 9504-11), and information to assist other police forces or agencies (Vol. 58, pp. 9597-9606). These instructions differed from those agreed to by the Executive Director of the U.I.C., who had agreed to provide information only when the act being investigated "gives rise to a good deal of public indignation". Assistant Commissioner Jensen expected that R.C.M.P. personnel would have exercised discretion as to when to seek information (Vol. 57, pp. 9439-43).

60. The next major development in R.C.M.P. policy resulted from an agreement with the Chief of Benefit Control of the U.I.C. By a memorandum of September 10, 1973, Commanding Officers were advised that "This is a confidential verbal agreement we have with the Special Investigations Committee and therefore it should not be widely publicized...". The ability to obtain information from the U.I.C. was not to be disclosed "to anyone outside the Force" (Vol. 57, pp. 9490-1).

61. The next document that gave rise to a change in policy was a memorandum of October 3, 1973, to the Commanding Officers of all field divisions and to the Director General of the Security Service (Ex. H-1, p. 63; Vol. 58, pp. 9506-7). This memorandum removed all restrictions concerning the crimes with respect to which the R.C.M.P. could seek information from the U.I.C. Assistant Commissioner Jensen testified that, although he was unaware of any particular document that supported his understanding that the U.I.C. had agreed to this change, this was his recollection as to what the Chief of Benefit Control had agreed to (Vol. 57, pp. 9507-8). There is evidence, however, that this officer of the U.I.C. expected that information would be given only in "major cases" (Ex. HC-1, p. 32), and that he preferred all requests to be made by R.C.M.P. Headquarters to the staff of the U.I.C. Special Investigation Committee. Headquarters, in a memorandum to Commanding Officers, stated that "any sub rosa arrangements which may exist" were not to be interfered with (Ex. H-1, p. 63; Vol. 58, pp. 9550-2). This memorandum represents the policy as it stood when we held hearings into this subject in June 1978.

62. Section 126(4) is capable of two interpretations, namely:

(a) the Commission has no authority to release information unless such authority is granted by regulations enacted by the Governor in Council; or

(b) the Commission has authority to release information unless the Governor in Council enacts regulations to limit this authority.

63. Both these interpretations give rise to other problems of interpretation concerning the meaning of "accurate" identification of individuals. Is this phrase intended to help the Commission or law enforcement bodies in determining whether the individual using the card is entitled to do so under the provisions of the statute? Or is the phrase intended to help in the general identification of persons for any reason whatsoever? The former interprets the purpose of section 126 (4) as related solely to the use of S.I.N. information or cards in the social security system. This is supported by the evidence: the S.I.N. "... has been developed solely in connection with social security programs" (Ex. H-11).

64. The second interpretation of the phrase "accurate identification of individuals" would allow release of information, not only to law enforcement agencies but also to banks, retail stores, credit agencies, and any other persons or organizations. This broader meaning could be rationally supported if one believes that the legislators in 1971 accepted the following: that S.I.N. had become a national identification system and, consequently, that use of S.I.N. or a S.I.N. card was for purposes some of which went beyond the social security system.

65. If the correct interpretation is that the information can be released only for accurate identification of individuals or the effective use by individuals of S.I.N. numbers and cards, both for purposes of the statute, then the release of the Central Index information by the Commission staff to the R.C.M.P. subsequent to the Unemployment Insurance Commission Act, 1971, was contrary to law unless it was released for the purpose of enforcing the provisions of that statute.

66. Even if the broader interpretation, i.e., the identification of individuals for any purpose whatever, is correct, a legal problem exists. It is clear on the evidence that the 1972 and 1973 arrangements, which we shall describe shortly, contemplated the release of information to the R.C.M.P. for the investigation of either certain specified crimes or "crime" generally. The evidence before us shows that the use of the information was not restricted to "the accurate identification of individuals" or to the investigation of breaches of the Unemployment Insurance Commission Act. True, in some cases, the information was used by the R.C.M.P. to identify dead bodies and the use of a S.I.N. Card by a person other than the person to whom it was lawfully issued. However, it was also used in a considerable number of cases to locate wanted persons and in this regard was described by Assistant Commissioner Jensen as a necessary tool in the location of fugitives — "people who are sought on criminal grounds" (Vol. 57, pp. 9318, 9286, 9324; Vol. 58, p. 9657).

67. On May 10, 1973, the R.C.M.P. advised their personnel that the fact that it could obtain information from the U.I.C. was not to be disclosed to outside agencies or police departments and that any requests for information from these bodies were to be denied (Ex. H-1, p. 55). This policy was in effect confirmed by the memorandum of September 10, 1973, which has already been mentioned. It is therefore surprising that the evidence discloses that after 1973 the R.C.M.P. used its arrangement with the U.I.C. to provide information to other domestic and foreign agencies and police departments. There is no evidence that the U.I.C. or its employees did not know that the arrangement was being used for those purposes. The evidence is that the U.I.C. did itself provide information to outside agencies and other police forces prior to 1971 but not thereafter.

68. A further legal issue raised by section 126(4) is as follows. It provides that "The Commission may... make available such information... to *such persons* as the Commission thinks appropriate to accomplish such purpose". Can the Commission or its employees be said to have exercised its discretion if

it was unaware of the identity of the recipient of that discretion? We think it cannot.

69. A further legal problem arises on the facts. The R.C.M.P. was provided with information from regional offices of the U.I.C. from the beginning of the U.I.C. programme in Canada to June 12, 1978 (Vol. 57, pp. 9289-90, 9324-5). From at least 1972 onwards there is no suggestion on the evidence that the arrangements negotiated with U.I.C. personnel related to anything other than Central Index information: the obtaining of information from regional offices after 1972 was not according to any agreement with U.I.C. personnel. As a result the release of this information cannot possibly be said to have been provided for under section 114 or its predecessor, unless one interprets that section as permitting the release of information by *an employee* of the Commission — an interpretation which we think is unsound.

1977

70. Effective August 15, 1977, the statute was amended by the Employment and Immigration Reorganization Act,[14] (the "Reorganization Act"). It created a department known as the Department of Employment and Immigration, under the jurisdiction of the Minister of Employment and Immigration. Pursuant to this Act, section 114 was amended in one significant particular: responsibility for determining which "other persons" may share information under that section is now assigned to the Minister of Employment and Immigration. Thus, the concluding language of the confidentiality provision in section 114 now reads "and such other persons as the *Minister* deems advisable". (The emphasis is ours.) Moreover, the section now applies to information collected both by the Unemployment Insurance Commission and the Department of Employment and Immigration. The section authorizes release of that information to employees of the Commission *or the Department of Employment and Immigration* in the course of their employment and "such other persons as the *Minister* may advise". (The emphasis is ours.)

71. The terms of section 126(4) were, however, identical in the amendment. Thus, the Commission remains vested with the discretion to determine "such persons" as are appropriate to accomplish the "purpose" set out in section 126(4). While the comments previously made concerning section 126(4) continue to apply with respect to section 114, regard must be paid to a new delegation of authority section introduced by the Reorganization Act. Section 5(2) provides as follows:

> Except as provided in any other Act of Parliament the Minister may, by order, authorize any officers or employees of the Department [of Employment and Immigration] or the Canada Employment and Immigration Commission established by section 7 to exercise powers or perform duties and functions of the Minister and any such officers or employees or classes thereof specified in the order may exercise the powers or perform the duties and functions mentioned in the order.

[14] S.C. 1976-77, ch.54, assented to August 5, 1977.

Thus, section 5(2) permits the Minister to delegate the discretion he has under section 114 to the Commission or to the Department or to employees of either body. Such employees or classes of employees must, in accordance with the terms of section 5(2), be expressly designated in the Minister's order and, further, the powers or duties and functions to be performed by them must also be expressly referred to in the order.

72. There is no longer any doubt that the Commission may delegate its power of decision. On the other hand, the new power of delegation excludes any possibility that an employee of the Commission could lawfully release information in the absence of an express delegation. This conclusion is further supported by the provisions of section 13(3) of the Reorganization Act, which empowers the Commission, by order, to authorize:

> (i) any officers or employees or classes of officers or employees of the Commission,
>
> or
>
> (ii) with the approval of the Minister, of the Department,
>
> to exercise powers or perform duties and functions of or delegated to the Commission.

73. Section 9(2) of the Reorganization Act reads as follows:

> The Commission shall comply with any directions from time to time given to it by the Minister respecting the exercise or performance of its powers, duties and functions.

This section is relevant to the Commission's authority under section 126(4). It permits the Minister to direct the Commission to release information under section 126(4) provided always that the release is for the purposes set out in that section.

74. We have been advised that, since the present Act came into effect in 1977, the Minister of Employment and Immigration has not delegated his authority under section 114 to the Commission or the Department or their employees, or issued any direction to the Commission pursuant to section 9(2) with respect to the release of information pursuant to section 126(4). Finally, there is no evidence before us to suggest that the Commission in turn has sub-delegated its discretion under section 126(4) to any of its own employees, to the Department or to employees of the Department. Consequently, if there was no such sub-delegation by the Commission, in our opinion any release of information between August 15, 1977 and the cut-off of information imposed on June 12, 1978, may have been in violation of the statute.

75. On June 12, 1978, a representative of the Canada Employment and Immigration Commission advised the D.C.I. that the Force's access to Central Index Information was terminated (Vol. 57, p. 9240). The extent of the restriction on the information flow and the reason for the restriction is found in an excerpt from the House of Commons debates of June 21, 1978, which reads as follows:

> Mr. Bill Clarke (Vancouver Quadra): Mr. Speaker, my question is for the Minister of Employment and Immigration. I want to ask him about the

recently revealed refusal to supply unemployment insurance information to the R.C.M.P. In view of the fact that this information has been supplied for many years, in spite of the regulation regarding the confidentiality of unemployment insurance information, I ask what type of confidential information was supplied to the R.C.M.P. and under what authority was that information given?

Hon. Bud Cullen (Minister of Employment and Immigration): Mr. Speaker, the legal opinion I received recently indicated that in the past the information given to the R.C.M.P. went beyond that which was allowed under section 126. This was a legal interpretation of that section. It seems to me that it is open to interpretation. Because we wanted to get the matter clarified, it seemed the wisest policy was to issue instructions that information other than that for the administration of the Unemployment Insurance Act or the administration of social insurance numbers should not be released until we had clarification of section 126. I am happy that the McDonald Commission is looking into this particular area to give us advice either that we do have authority to give additional information as the minister shall determine, or that we should amend legislation to do what I think is appropriate, that is, to give this information to the R.C.M.P. to help their investigations.

Mr. Clarke: Mr. Speaker, I ask the minister what recent developments caused the ruling to be investigated and forced the government to stop giving that information.

Mr. Cullen: Mr. Speaker, until the carping of opposition members, we used what we thought was common sense and tried to help the R.C.M.P. in their fight against organized crime.

An hon. Member: Organized crime?

Mr. Cullen: I might say that with the passage of Bill C-27, the hon. member's colleague, the hon. member for Hamilton West, quite correctly thought that the minister should have the responsibility for giving information under the Unemployment Insurance Act to other people, and insisted that the wording be changed from "the commission" to "the minister" so that the minister had to accept responsibility. I sought a legal opinion to determine whether we were acting within the provisions of section 126. The advice I have from legal counsel is to the effect that more information is being provided than was authorized by that section. Because of that, I have ordered it stopped.[15]

76. For the reasons given above our conclusion is that throughout the three decades since 1946, the R.C.M.P. has obtained information from the staff of the U.I.C. by means which, through a failure to take advantage of the statutory provisions specifying the power of deciding upon access, have violated the confidentiality provisions of the legislation.

Extent and prevalence of access by the C.I.B. to U.I.C. data

77. The R.C.M.P. maintained Request for Information files from 1974 to April 1978. These files were created as a result of the 1973 arrangement and were maintained to record the requests that were made following the time of

[15] House of Commons, *Debates*, June 21, 1978, p. 6619.

that arrangement (Vol. 58, p. 9564). The requests for information made by the C.I.B. to the U.I.C. for the period 1974 to 1978 were as follows:

1974	—	265
1975	—	92
1976	—	544
1977	—	648
1978 (to April)	—	74
		1,623

Of the 648 requests for the year 1977, between 250 and 266 related to the investigations of U.I.C. frauds. Accordingly the number of non-U.I.C. related offences for 1977 was approximately 400 and for the period 1974 to April of 1978 was approximately 1,370 (Ex. H-7A; Vol. 60, pp. 9664-7). A review of the relevant files for the year 1976 and 1977 indicated as follows:

	Non-U.I.C. Recorded Requests	Reason for Request Not Indicated
1976	399	268
1977	428	313

78. The R.C.M.P. advised us that the request files are incomplete, and that the reason for the requests may have been communicated in a different fashion, for instance by telephone, by correspondence, or by reference to a particular case file. However, that information cannot be determined with any certainty at the present time (Vol. 58, pp. 9671-2).

79. The request files for the period 1974-78 indicate that other police forces and other agencies contacted the Commercial Crime Branch Headquarters computer terminal directly to make use of the 1973 arrangement. These included requests that were acted on from the following bodies, which are named here to illustrate the broad range of domestic and foreign forces and agencies whose requests were processed:

(a) Ingersoll Police Force
(b) Quebec Provincial Police Force
(c) Temagami Police Force
(d) Indiana State Police
(e) Winnipeg Police Force
(f) Medicine Hat Police Force
(g) York Regional Police Force
(h) Sudbury O.P.P.
(i) Kingston Police Force
(j) Burlington O.P.P.
(k) U.K. Customs
(l) Canadian National Railway Police
(m) D.N.R. — Collections Department

(Vol. 58, pp. 9600-4.)

D. OTHER FEDERAL GOVERNMENT DEPARTMENTS AND AGENCIES

(a) *Department of Industry, Trade and Commerce: the Industrial Research and Development Incentives Act*

80. Under the Industrial Research and Development Incentives Act,[16] known as I.R.D.I.A., the Minister of Industry, Trade and Commerce may authorize the payment of a development grant to a corporation for scientific research and development. A corporation applying for such a grant must provide such information as is specified by regulation and prescribed by the Minister. A statutory "privilege" is created by section 13, and disclosure of information contrary to section 13 is made an offence.

> 13. All information with respect to a corporation obtained by an officer or employee of Her Majesty in the course of the administration of this Act is privileged, and no such officer or employee shall knowingly, except as may be necessary for the purposes of sections 11 and 12 or in respect of proceedings relating to the administration or enforcement of this Act, communicate or allow to be communicated to any person not legally entitled thereto any such information or allow any such person to inspect or have access to any application or other writing containing any such information.
>
> 15.(2) Every officer or employee of Her Majesty who contravenes section 13 is guilty of an offence punishable on summary conviction.

Can the R.C.M.P. obtain access to such information? The references to sections 11 and 12 are irrelevant for our consideration as they relate to information obtained from the Minister of National Revenue or provided to that Minister. But what is the scope of the phrase "proceedings relating to the administration or enforcement of this Act", and when are members of the R.C.M.P. "legally entitled" to such information?

81. In 1974, the Commercial Crime Branch of the R.C.M.P., during the course of an investigation, wrote to the Deputy Minister of Industry, Trade and Commerce to obtain information concerning I.R.D.I.A. grants made by the Department to two firms. Apart from the existence and amount of grants, the Deputy Minister declined to provide information because of the provisions of section 13 of the Act. This resulted in contradictory legal opinions being given by the Legal Branch of the R.C.M.P. and by the Legal Services Branch of the Department. Finally, in May 1975, the Assistant Deputy Attorney General gave a written opinion that the Department may not, except pursuant to the exceptions contained in section 13, reveal to the R.C.M.P. information obtained under the statute. The Deputy Minister considered that opinion to be binding upon the Department but expressed willingness to co-operate by formally requesting an investigation pursuant to section 13 if the R.C.M.P. has information indicating possible irregularities in the administration of I.R.D.I.A.

---

[16] R.S.C. 1970, ch.I-10.

82. Such willingness to co-operate would apply only if the investigation related in a direct fashion to the Act. However, the investigation in question, in which the governing opinion was that information could not be provided, was under the Criminal Code. It concerned an allegation that an individual received a percentage of an I.R.D.I.A. grant in return for exercising his influence with the Government of Canada in regard to the application for the grant.

83. It appears from the documents before us (Ex. N-1) that on another occasion in 1974 a member of the Commercial Crime Branch conducting another investigation did obtain "complete access" to information in the files of the Department of Industry, Trade and Commerce, which had been obtained under I.R.D.I.A. There is no other evidence before us to indicate the extent and prevalence of such access. However, the Officer in Charge of the Operational Task Force (the group in the R.C.M.P. charged with tasks relating to this Commission of Inquiry and others) reported to us by letter dated November 21, 1978, that there was one case in 1975 in which there was an investigation of a possible "kick back" in regard to an application; that case resulted in the above-noted opinion being given by the Department of Justice. He added:

> Due to the fact that C.C.B. (Commercial Crime Branch) investigation files were not categorized by Government Departments, it would require a review of almost all Commercial Crime Branch files to determine if they dealt with an I.R.D.I.A. investigation. From speaking to members of C.C.B. they cannot recall any other case involving I.R.D.I.A.

We concluded that the time and cost of undertaking such a massive search were not warranted in the circumstances.

(b) *Department of National Health and Welfare: Family Allowances and Old Age Security*

84. Section 32 of the Family Allowances Regulations, 1954-1508, provided as follows:

> Except where required by law or when necessary for the administration of the Act or these regulations, no person who obtains information under the provisions of the Act or these regulations shall disclose or communicate such information or allow it to be disclosed or communicated.

85. The Family Allowances Act was repealed and replaced by The Family Allowances Act, 1973.[17] The confidentiality provision is now found in section 17 of the statute which provides as follows:

> (1) Except as provided in this section or section 18, all information with respect to any individual obtained by the Minister or an officer or employee of Her Majesty in the course of the administration of this Act and the regulations or the carrying out of an agreement entered into under Section 18 is privileged and no person shall knowingly, except as provided in this Act, communicate or allow to be communicated to any person not legally entitled thereto any such information or allow any person not legally entitled thereto to inspect or have access to any such information.

[17] S.C. 1973-74, ch.44.

The communication of such information contrary to section 17 is an offence:

> 20. (1) Every person who knowingly
>
> (e) contravenes section 17 by communicating or allowing to be communicated to any person privileged information or by allowing any person to inspect or have access to any statement or other writing containing any such information is guilty of an offence and liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding one thousand dollars or both.

However, subsection (2) provides a number of exceptions when information obtained by the Department in the course of the administration of the Act may be communicated to persons outside the Department. These exceptions are the Department of Indian Affairs and Northern Development, the Department of Manpower and Immigration, the Department of National Revenue, the Department of Supply and Services, the Unemployment Insurance Commission and Statistics Canada. The prohibition found in subsection (1) is also expressly not applicable to "proceedings relating to the administration and enforcement of this Act". Section 18 empowers the Minister to enter into an agreement with the government of a province under which the Minister may furnish to the government of a province any information which has been provided by a person who has applied for family allowances.

86. The "Minister" referred to in that Act is the Minister of National Health and Welfare. He is also the Minister referred to in the relevant provisions of the Old Age Security Act,[18] which have been in force since the Statutes of 1966-67. A similar prohibition was previously found in paragraph 3(1)(a) of the Regulations made pursuant to the previous Old Age Assistance Act. In that statute the confidentiality provision is found in section 19(1) which reads as follows:

> (1) Except as provided in this section, all information with respect to any individual applicant or beneficiary or the spouse of any applicant or beneficiary, obtained by an officer or employee of Her Majesty in the course of the administration of this Act is privileged, and no such officer or employee shall knowingly, except as provided in this Act, communicate or allow to be communicated to any person not legally entitled thereto any such information or allow any such person to inspect or have access to any statement or other writing containing any such information.

Subsection (2) provides a number of exceptions when information obtained by the Department pursuant to the Act or the regulations may be communicated outside the Department. These exceptions are the same Departments of the federal government as those referred to in the Family Allowances Act except that the Departments of Finance and Veterans' Affairs are added and the Departments of Indian Affairs and Northern Development and of Manpower and Immigration are not included. Information may also be provided to any provincial authority administering a programme of assistance payments. The prohibition found in subsection (1) is expressly not applicable to "proceedings relating to the administration or enforcement of this Act".

---

[18] R.S.C. 1970, ch.O-6.

87. The R.C.M.P. has long sought access to information provided to the Minister of National Health and Welfare by a parent applying for family allowances or a person applying for old age security. This information has been sought in order to assist individuals who have asked for the help of the R.C.M.P. in locating missing relatives and foreign embassies seeking persons, although the policy has been that, if such information is obtained, the person or embassy making the inquiry is not to be given the information if the "missing" person objects.

88. The R.C.M.P. has also sought the information in criminal investigations. For example, where a person suspected of a crime has vanished with his wife and children, information as to the address to which family allowance cheques are sent at the request of the parents may be of considerable assistance in enabling the police to locate the suspect.

89. In December 1954 R.C.M.P. Headquarters asked the Department of Justice for an opinion as to whether the furnishing of information to the Force to assist it in locating missing persons violated the "security" provisions of the Acts and regulations governing family allowances, old age security and old age assistance. In January 1955 the Deputy Attorney General, Mr. Varcoe, gave his written opinion that the provisions of the statutes and regulations

> preclude the giving of the information referred to therein to R.C.M. Police officers to assist them in locating missing persons. These prohibitions apply notwithstanding the manner in which a recipient proposes to deal with the information.

90. Consequently, in March 1955, a written instruction was sent to all divisions, sub-divisions and detachments. This advised of the ruling received from the Department of Justice. It then directed that members of the Force conducting enquiries as to the whereabouts of wanted or missing persons must not approach any regional office for information from the family allowances or old age security records. The instruction was entitled "Temporary" and was "to be withdrawn September 1, 1955". It was sent out as a "Temporary Instruction"

> . . . as it is felt that in six months time personnel in the field will be familiar with the fact that no information can be obtained from this Division of the Department of National Health and Welfare and a temporary instruction will have served our purposes.

91. In 1968 the officer in charge of the Commercial Fraud Section urged that an effort be made to overcome the "roadblock" created by the prohibition against disclosure that was then contained in a regulation under the Family Allowances Act, either by the Deputy Minister or another senior officer of the Department authorizing disclosure as a matter of policy, or by having the regulation amended. In order to prepare for an approach to the Department, the then Officer in Charge of the Criminal Investigation Branch, Superintendent M.J. Nadon, wrote to the Commanding Officers of the divisions to ask:

> which Divisions are suitable to acquire information through confidential sources within these Divisions

despite "the fact that they are statute [sic] barred by secrecy provisions within their regulations". The letter added:

> If we are receiving more co-operation at present than is apparent at this Headquarters, we may avoid any contact with the Department if we feel that such action would only serve to eliminate existing sources.

In reply, several commanding officers reported that information was being provided by confidential sources within the Department. Of these, the report from Alberta, by Detective Inspector T.S. Venner, explained that the assistance was being provided without the knowledge of the "national headquarters" of the Department and that he had been assured that "any official approach along these lines at Ottawa would only serve to eliminate these sources". The report from Manitoba was made by the member who obtained information from the Departmental source. It observed that the source had told him that the Regional Director of the Department

> continually brings to their attention the security aspects of their work and threatens dire results should there be any breach of same.

92. There is no indication that at that time any approach was made by R.C.M.P. Headquarters to the Department of National Health and Welfare. We infer that no approach was made for fear of affecting adversely the successful relationships that had been developed with sources within the Department in several provinces.

93. In November 1978 the Operational Task Force of the R.C.M.P., which had been created to carry out tasks related to Commissions of Inquiry, reported to us that it had conducted a survey of all divisions to determine whether local arrangements were in effect enabling members of the Force to obtain family allowance information. The divisions generally replied that as far as they could ascertain there did not exist any confidential arrangements with the Family Allowances Division of the Department. However, four cases were reported in which approaches were made by the Force to the Family Allowances Division other than in regard to the administration of the Family Allowances Act.

(i) In an investigation of the abduction of a seven-year-old child, the approach was made to determine whether a new application had been made for family allowance in regard to the abducted child. The Department advised that no new application had been made. (The mere disclosure that an application had or had not been made would not be prohibited.)

(ii) In 1970 co-operation was received in regard to a murder investigation. No further details were given.

(iii) A contact was made with the local office in an investigation under the Immigration Act. No further details were given.

(iv) A request was made in a fraud investigation. It does not appear that any information was given out, the disclosure of which would be prohibited.

Those cases illustrate the variety of situations in which information would be of assistance in criminal investigations.

(c) *Foreign Investment Review Agency*

94. The Foreign Investment Review Agency (F.I.R.A.) was established pursuant to the provisions of the Foreign Investment Review Act.[19] The Agency is empowered to advise the Minister concerning applications for the sale of control in Canadian business enterprises to non-Canadians, or the establishment of a new business in Canada by non-Canadians. In the case of the sale of an existing business, the applicant is the Canadian business enterprise. The applicant must provide the Agency with detailed information about the Canadian business enterprise or the new business. Section 14(1) of the Act is the confidentiality provision, violation of which is an offence:

> 14. (1) Except as provided in this section, all information with respect to a person, business or proposed business obtained by the Minister or an officer or employee of Her Majesty in the course of the administration of this Act is privileged and no person shall knowingly, except as provided in this Act, communicate or allow to be communicated to any person not legally entitled thereto any such information or allow any person not legally entitled thereto to inspect or have access to any such information.

The only exception provided for in the remainder of the section, which could in any circumstances enable the R.C.M.P. to have access to such information, is in respect of "legal proceedings relating to the administration or enforcement of this Act".[20] (Even that exception may not permit disclosure until after an information has been laid.)

95. In 1977, in a major international fraud investigation relating to "finder's fees", the R.C.M.P. attempted to obtain information from F.I.R.A. but F.I.R.A. personnel refused to provide the information on the ground that it was confidential. This illustrates that it is in the investigation of commercial fraud cases that F.I.R.A.'s information would be useful. Later that year the R.C.M.P. recorded that an arrangement had been made orally to deal with requests by the R.C.M.P. for information "unofficially, on a case by case basis". The arrangement entered into appears to us to have contemplated the furnishing of information in violation of the Act. However, so far as we have been able to ascertain the R.C.M.P. has not since then obtained any such information.

E. NEED AND RECOMMENDATIONS

96. In Part X, Chapter 5, we shall recommend that the R.C.M.P., for criminal investigation purposes, should have access to all personal information held by the federal government with the exception of census information collected by Statistics Canada. This access will be subject to a rigorous set of controls and review. Specifically we shall propose that R.C.M.P. access to personal information other than of a biographical nature be through a system of judicially granted authorizations subject to the same terms and conditions as are now found in section 178 of the Criminal Code with regard to electronic surveillance.

---

[19] S.C. 1973-74, ch.46.

[20] Section 14(4)(a).

CHAPTER 6

ACCESS TO AND USE OF CONFIDENTIAL INFORMATION HELD BY THE FEDERAL GOVERNMENT — SECURITY SERVICE

A. ORIGIN, NATURE AND PURPOSES OF PRACTICES

1. Members of the Security Service consider that important aspects of their work have been helped by having access to government information about individuals. Persistent efforts have been made to develop sources within government departments, whether in Ottawa or at some other centre. The Security Service members who developed these sources were, so far as can be determined from examination of the files, usually quite conscious that the sources would be breaking the law by contravening provisions of statutes concerning confidentiality of information. However, the Security Service considered that such information was needed to protect the security of Canada, and would be difficult and often impossible to obtain by other means. The sources themselves agreed to provide the information for entirely unselfish motives, being persuaded of the desirability and necessity of providing this form of assistance to the R.C.M.P.

2. As with the C.I.B. in Chapter 5, we shall examine the extent to which the Security Service gained access to several distinct sets of government records.

B. DEPARTMENT OF NATIONAL REVENUE

Policy and implementation

(a) *History*

3. During the Second World War, a regulation[1] made pursuant to the War Measures Act on July 30, 1940, made it mandatory that the Commissioner of Income Tax allow the R.C.M.P. to have access to any information contained in any return or other written document furnished under the provisions of the Act. This regulation was revoked on July 23, 1946.

4. Nevertheless, it appears that the Special Branch (which later became the Security Service) continued to have access to such information. On September 12, 1951, Superintendent (later Commissioner) McClellan advised the R.C.M.P. divisions across the country that thenceforth inquiries, which previ-

[1] P.C. 3563.

ously had apparently been directed to district offices of the Income Tax Branch, should be directed to R.C.M.P. Headquarters, so that Headquarters might ask the Income Tax Branch for information regarding the financial structure of an organization or the circumstances of an individual. Superintendent McClellan stated that the Income Tax Branch had indicated that statutory restrictions on the dissemination of information contained in Income Tax Branch files made the matter "rather delicate, not only from the legal viewpoint, but because of the fact it places employees of that branch in a rather difficult position".

5. Although there are no details in R.C.M.P. files of the relationship during the next 15 years, a memorandum on October 5, 1967, from an R.C.M.P. officer to the Director of Security and Intelligence, Assistant Commissioner Higgitt, stated that in November 1966, the Security and Intelligence Directorate's source in the Department of National Revenue had become increasingly concerned about co-operating with the R.C.M.P. The source had based his unwillingness to continue his co-operation on the fact that he was contravening the provisions of the Income Tax Act. The memorandum concluded that the source had been uncooperative for several months and appeared to be no longer available. Until this time, according to another memorandum, the source had provided information as to taxpayers' financial standing and other data which appeared on income tax returns. In this memorandum, the officer again recognized that a source, by co-operating, would be in contravention of section 133 of the Income Tax Act. On January 19, 1968, this officer wrote a memorandum in which he accepted that the provision of such information clearly resulted in a contravention of the Income Tax Act, and therefore it would be undesirable to obtain a ruling from the Department of Justice which could only state that the R.C.M.P. was excluded from obtaining the information. That, according to the officer, would then place the Security and Intelligence Directorate in the position that, if it carried on as it had in the past, it would be doing so "in contravention of a recent and explicit ruling from the legal officer of the Crown".

6. On October 24, 1969, after publication of the Report of the Royal Commission on Security, an R.C.M.P. memorandum suggested that renewed efforts should be made to establish liaison with the Department of National Revenue (Income Tax and Canada Pension Plan Divisions) and the Department of National Health and Welfare, "making the necessary submissions through the Solicitor General".

7. A memorandum by an R.C.M.P. officer dated November 18, 1969, noted the following passages in the Report of the Royal Commission, pertaining to the R.C.M.P.'s general relations with government concerning security matters:

> We have little sympathy with the more extreme suggestion that inquiries about persons should not be undertaken because of the individual's 'right of privacy', nor with the view that the process of personnel investigation by the State is alien to normal and democratic practice.

> Neither does an individual have a right to confidence; on the contrary, access to classified information is a privilege which the State has a right and duty to restrict.[2]
>
> Although the role of the R.C.M.P. is admittedly ill-defined, and recognizing that government policy has been inhibiting, we are not sure that the RCMP has made a sufficient, or a sufficiently sophisticated effort to acquaint the government with the dangers of inaction in certain fields. We are left with the impression that there has been some reluctance on their part to take desirable initiatives and some inadequacy in stating the case for necessary security measures in interdepartmental discussions at the higher policy-making levels.[3]

Obviously in these passages the Royal Commission intended to suggest that the R.C.M.P. should, in formal discussions of policy and amendments to legislation, be aggressive in emphasizing its need for information that would ordinarily be protected: the Royal Commission did not imply that the R.C.M.P. should make informal arrangements to obtain information by practices that resulted in violations of provisions of statutes.

8. However, it appears that even before that suggestion of such a formal approach was made, the Security Service had taken its own initiative. According to a November memorandum, the Service had, "in recent months, established a rather tenuous and highly restricted relationship with [source X] of the Income Tax Branch". (X is the name given by this Commission to a member of the Department of National Revenue, Income Tax Branch, who testified voluntarily to the Commission *in camera*. While much of that testimony was made public, the identity of X has been carefully protected by the Commission.) The memorandum continued that there was "the feeling that we cannot use this source to the degree that should be possible under more relaxed conditions, preferably generated from a more senior level". The memorandum also questioned the suggestion made of an approach through the Solicitor General, on the grounds that involving the Solicitor General would imply an attempt to amend the Income Tax Act, which would be self-defeating in that it would likely produce publicity, and that an unfavourable ruling by the Solicitor General would "effectively prevent us from subsequently attempting any alternative route". The memorandum suggested as an alternative that an approach be made to the Deputy Minister of National Revenue.

9. On November 25, 1969, in a note to the Director of Security and Intelligence, Assistant Commissioner Higgitt, it was recommended that Mr. Higgitt approach the Deputy Minister of National Revenue to explain the problem. If the Deputy Minister could not co-operate, the Security and Intelligence Directorate would somehow have to obtain the Solicitor General's good offices to intercede with the Minister of National Revenue. The note stated that "to continue efforts at any lower level simply puts these individuals on the spot". There is nothing in R.C.M.P. files to indicate that any meetings took place at or following that time between the Security and Intelligence

---

[2] *Royal Commission on Security*, 1969, paras. 79 and 80.

[3] *Ibid.*, para. 56.

Directorate and officials of the Department of National Revenue to establish a regularized practice of providing information to the Security and Intelligence Directorate.

10. While all these approaches were being exchanged, the relationship of the Security and Intelligence Directorate with X had been established. X received requests for two types of information: the first was "tombstone data", meaning such biographical information as the name and address of the taxpayer and his place of employment; the second was financial information. X agreed to provide information because X was convinced that it was necessary for the security of Canada. X's evidence was that X did not seek or obtain the approval of superiors, but acted independently, and we accept this evidence. X made the arrangements at a luncheon with R.C.M.P. officers, who explained the difficulties the R.C.M.P. were having in obtaining information about a certain class of persons of interest to the Security and Intelligence Directorate. X insisted that all requests be carefully screened prior to submission to X, that one R.C.M.P. officer deal only with X, that no communication be on paper so that no one in the Department would know what was going on, and that any information X gave to the R.C.M.P. officer not be disseminated outside the Security and Intelligence Directorate.

11. X testified to being aware of the provisions of Section 241 of the Income Tax Act. With respect to the tombstone data it had always been X's opinion that such information did not fall within the restrictions found in the section. With regard to financial data concerning the taxpayer, X was doubtful that providing the information was legal, and because of these doubts had insisted that all communications be oral. X did not anticipate that the Department of National Revenue would obtain any tax benefit in return for the release of tax information to the Security and Intelligence Directorate. X was unaware that at the time there was any consideration being given within the Security and Intelligence Directorate to obtaining official approval for access to tax information, and did not know that representations were being made by the R.C.M.P. concerning the matter.

12. The R.C.M.P. officer asked for and obtained, not only information which X could obtain from the computer, but also information which could only be obtained from the field. X recalled that this probably included information as to the source of income. In X's opinion, the Department of National Revenue should not be officially engaged in passing information on these grounds "because one of the cornerstones [of the administration of the Income Tax Act] was that we kept our files confidential". X testified that no one in the Department of National Revenue at that time knew that X was passing information to the R.C.M.P. Security Service. As far as X knew, no one other than the R.C.M.P. contact or the previous R.C.M.P. contact knew of X's identity as a source for the Security Service.

13. X told us that the Department's firm policy was to co-operate with no one at all unless there were legal grounds for doing so. If asked whether the Department could enter into an agreement with the Security Service or have anything to do with the provision of information to the Security Service, X's

advice would have been that that could not be done. Nevertheless, after listening to what the R.C.M.P. contact said, X felt prepared to accept the responsibility and risk of passing information, since the reasons for not passing information were outweighed by the difficulties the police were having in obtaining this type of information for what X considered "the security of the country".

14. X said that this was according to X's "own conscience, and my own belief in what Canada represented" and "that whatever it was, I wanted to protect that". X could foresee no tax advantage, and regarded the relationship not as being reciprocal, but rather as a one-way street. X acted out of a "sense of national duty". X admitted that when an individual in the Department of National Revenue decides in the interest of what he or she conceives a higher duty to the state, to give information obtained under the Income Tax Act to some body such as the police, "it certainly weakens the Department's image" and weakens the public confidence that tax information will be kept confidential. X never sought or received any payment for the services given to the Security Service, other than occasional lunches, and does not regret having made the decision to assist the Security Service.

15. We shall return to X later, but first it is necessary to refer to the evidence before us as to whether, in 1970, an agreement was made between another official of the Department of National Revenue and the Security Service for the passing of such information to the Security Service. On September 4, 1970, the R.C.M.P. officer who contacted X addressed a memorandum to the Commissioner, to the attention of the Director of Security and Intelligence, concerning contact X. (The code number rather than the name was used.) The memorandum reported that the officer had continued to see X frequently as and when required, and that X continued to cooperate freely and willingly. The memorandum reported that, while X had theretofore insisted on dealing personally with the writer, X had, however, that day "quite spontaneously and without any prior discussion" introduced the R.C.M.P. contact to Y, another member of the Department of National Revenue. The memorandum recorded that X very briefly explained to Y the nature of the relationship and told Y that if X was not available the R.C.M.P. officer could pass inquiries to Y, and Y would extend the same co-operation. The R.C.M.P. officer recorded that Y "quickly grasped the delicate nature of the relationship" and indicated the co-operation would be forthcoming. Mr. Starnes says that he does not think that he was aware of this September 4, 1970, memorandum.

16. On September 15, 1970, Mr. Starnes, in a longhand memo to Superintendent Chisholm, said:

> I spoke to Commissioner about this matter on 3 September. He told me the Minister was opposed to joining with his colleague the Minister of National Revenue in a submission to cabinet. Could a 'blind' memo on the present state of play be prepared which I could use in talking to the Minister.

17. On September 23, 1970, a longhand note by Mr. Starnes to the Commissioner stated:

> If you see no objection I would like to show this memo to Minister on next occasion we see him to try and get action on question of access for S & I purposes to income tax records.

The memorandum in question is one which related to the use to which such information would be put by the Director of Security and Intelligence. In a longhand note at the bottom of the memorandum dated September 23, 1970, Commissioner Higgitt stated:

> I have raised this a number of times with the Minister and will do so again. He has not as yet been able to get the Minister of National Revenue to give his Department the necessary instructions to cooperate even though he seems to be favourably inclined himself. Mr. Côté is seemingly facing considerable opposition from his departmental officials. I will raise it again. I have retained a copy.

Mr. Starnes testified that he has no recollection of having raised the matter with Mr. McIlraith.

18. (It will be recalled that, in connection with criminal investigations, Commissioner Higgitt had written to Mr. McIlraith on March 20, 1970, advising him that representatives of the D.N.R. and the R.C.M.P. had finalized a draft agreement and a Memorandum to Cabinet.)

19. On September 8, 1971, X's R.C.M.P. contact addressed a memo to the Commissioner, to the attention of the Director General of the Security Service, with regard to X, identifying X by code number. The memorandum recorded that X's contact and another R.C.M.P. officer had entertained the source at lunch on September 7, 1971, and that the other R.C.M.P. officer had been introduced to the source. He also recorded that they discussed with the source

> . . . the fact that the Solicitor General had elicited agreement from [a public servant in] the Department of National Revenue to provide the Security Service with information from Taxation Records; Source was fully aware of this and told us how [the source] had explained to the [public servant] that the arrangement would have to remain unofficial due to lack of a legal base for passing such information. Source's view is that [the source] now has approval from the source's [superior] to do what [the source] has been doing for us on [the source's] own initiative for the past two years.

The memorandum also indicated that the Security Service should continue to deal directly with X only. According to the memorandum of September 4, 1970, X had introduced the writer to Y, who was to be used as an alternative only when X was not available. The writer believes that his memorandum accurately set forth what happened (Vol. 147, pp. 22714-5). In a further memo of September 8, 1971, the writer also stated that X

> insists on confining the arrangement to these few people as there is no legal base for this activity thus leaving [the source's] department in an indefensible position should wider knowledge of the arrangement cause a leak into the public domain.

20. X confirmed to us having been introduced to another R.C.M.P. officer by the R.C.M.P. contact and thinks it was at a lunch meeting. X recalled that the R.C.M.P. contact was leaving his position and another R.C.M.P. officer was to

replace him. However, X denied having discussed with the R.C.M.P. contact that the Solicitor General had elicited agreement from a public servant of the Department of National Revenue to provide the Security Service with information from taxation records. X denied having discussed the matter with the person in the Department to whom the memorandum referred (Vol. 147, p. 22672).

21. X testified that X never told any public servant what X was doing in respect of this matter, and had no recollection of introducing Y or making the arrangement that Y would be a substitute. We accept the facts as set forth in the memorandum written by X's contact. X further said that as far as X knows, no one in the Department knew that X was passing information to the Security Service (Vol. 147, p. 22656).

22. The consciousness of senior officers of the Security Service across Canada that the practice was illegal is demonstrated by their honouring the request of Headquarters that a memorandum of August 19, 1971, concerning access to taxation records be returned for destruction.

23. Despite attempts by the R.C.M.P. contact to have all requests for taxation information routed through Headquarters, it appears that Security Service members at the local level continued to use local sources in the Department of National Revenue. On February 24, 1972, an R.C.M.P. memorandum for file, written by X's contact, noted that

> From the number of incidents appearing from the field of our members inadvertently using long established local sources in this area it is obvious that we are not going to be able to 'turn off' the field Divisions in this area without taking unnecessarily large issues [sic] on the subject.

His memorandum records that he proposed to the Acting Deputy Director General, on February 16, 1972, that he discuss the matter with X and that if X agreed, the R.C.M.P. contact would tell the divisions that it would be in order to resume discreet use of the local sources. The R.C.M.P. contact records that the Acting DDG agreed, that he spoke with the source on February 17, 1972, and that the source agreed, saying that there was no "need for [the Security Service] to persist in trying to prevent [its] members from contacting their local contacts". Consequently, on February 24, 1972, the R.C.M.P. contact wrote to the Commanding Officers across the country, advising that the local Department of National Revenue sources could be used discreetly.

24. The official Security Service policy was recorded in the policy manual, on a page dated April 19, 1972, as follows:

Liaison with Income Tax Branch

> Due to statutory restrictions imposed on information contained in Income Tax files it is usually not possible to obtain the desired information from district tax offices. Headquarters *may* be in a position to assist in this regard provided the enquiry is sufficiently important and there are no other sources from which to obtain the information. The specific information desired concerning the financial structure of an organization or individual must be stated in the requests to Headquarters.

25. X continued as a source at the Department of National Revenue in Ottawa until replaced by another (Ex. GC-11).

Extent and prevalence

26. A Staff Sergeant who since 1971 has been attached to the Branch of the Security Service which has responsibility for programmes of developing "human sources" testified that between August 1971 and the fall of 1977 he was able to ascertain 132 instances in which information was obtained from income tax files. Of these, 52 involved X's co-operation. The balance were either through Headquarters (presumably through X's successor as source) or through local contacts. He believes that divisions kept records of access from August 1971, when they were informed that an agreement had been reached in Ottawa. In late 1977 the association with the "main source" in Ottawa was stopped by the Security Service handler. No instructions were sent by Headquarters to the divisional level that the members of the Security Service were to desist from obtaining such information, and there is no evidence as to what has occurred at the local level since the fall of 1977.

27. So far as can be ascertained, no payment was ever made to, or expected by, sources in the Department of National Revenue.

Legal issues

28. An exposition of legal issues, as applicable to the Security Service, would be no different than the discussion already set forth in regard to the C.I.B. in Chapter 5. There is no need to repeat what is developed there.

29. If a court, engaged as was the court in *Glover* v. *Glover*,[4] in applying the law as to the custody of children, is not a person "legally entitled" to the address of a taxpayer, we think that a member of the R.C.M.P. Security Service cannot be said to be a "person legally entitled" to biographical information or financial information disclosed on an income tax return. If this is so, the disclosures made by sources in Ottawa or elsewhere were offences by those persons under section 241, and if in any of the specific cases, a member of the R.C.M.P. "abetted" (encouraged) the sources, he was a party to the offence under section 21 of the Criminal Code. If he "counselled" or "procured" the source to commit it, he was a party to the offence under section 22 of the Criminal Code. We did not receive evidence as to such encouragement, counselling or procurement in specific cases. If the Attorney General of Canada considers that further investigation of specific cases is desirable with a view to considering whether there should be prosecution, he may begin his investigation with some specific cases of which details of a general nature are given in our records. However, we note that the substantive offence is a summary conviction offence; therefore there cannot be prosecution except within six months of the offence.

[4] [1980] D.T.C. 6262 (Ont. C.A.). This case is discussed in Part III, Chapter 5.

C. UNEMPLOYMENT INSURANCE COMMISSION

Security Service Policy

1950-1964

30. Co-operation and information exchange between the Unemployment Insurance Commission and the Security and Intelligence Directorate of the R.C.M.P. initially developed out of the arrangements entered into between the C.I.B. and the U.I.C. Until 1956 the Special Branch (predecessor of the present Security Service) was part of the C.I.B. In 1956 it became the Directorate of Security and Intelligence and ceased to be part of the C.I.B. However, it "piggy-backed" on the C.I.B. arrangements to obtain biographical data and other information collected by local offices of the U.I.C. (Ex. H-1, p. 134; Vol. C16, pp. 7852-3).

31. It will be recalled from our narrative in Part III, Chapter 5, that the Deputy Commissioner of the Force wrote to the Commanding Officers of all divisions on June 11, 1964, to advise that the Commissioner of the Force had assured the Minister of Justice that the Force did not intend to seek access to confidential data which would be collected under social security legislation then before Parliament, and that members of the Force were therefore not to seek access to information accumulated by the U.I.C. under this programme (Ex. H-1, p. 16). This memorandum, a copy of which was circulated to the Director of Security and Intelligence, and retained in the files of the Security and Intelligence branch in Toronto, contained the following admonition: "This is forwarded for your information. Please see that all members under your command comply with the Deputy Commissioner's instructions" (Vol. C16, pp. 1861-2; Ex. HC-1, p. 72). However, as we have also seen, the Deputy Commissioner wrote a further letter on June 25, 1964, just two weeks later, instructing that access to U.I.C. records was to continue.

1964 to 1971

32. From August 1964 to March 1971, the Security and Intelligence branch at "A" Division in Ottawa had its own direct, person-to-person working relationship with a U.I.C. representative, pursuant to which the branch, through this representative, could gain access to the Master Index and obtain information from regional offices of the U.I.C. (Vol. C16, pp. 1858-60; Ex. HC-1, p.1). There was no arrangement between the Security and Intelligence Directorate at Headquarters and the U.I.C. during this period, although Headquarters was aware of the "A" Division arrangement (Vol. C16, pp. 1875, 1891-2). There is no indication on the evidence that the Security and Intelligence branch of any other division had such an arrangement with the U.I.C. during this period (Vol. C16, pp. 1863, 1870, 1872).

33. In March 1971 this flow of information to "A" Division was all but cut off by the U.I.C. in light of "questions in the House of Commons". Following this restriction the U.I.C. continued to supply a social insurance number when "A" Division could provide a name (Ex. HC-1, p. 8). This "cut-off" of information resulted in an exchange of correspondence at the ministerial level

between the Honourable Jean-Pierre Goyer (the Solicitor General) and the Honourable Bryce Mackasey (the Minister of Labour) following which meetings were arranged between U.I.C. and Security Service representatives to discuss the resumption of the flow of information.

1972 to 1978

34. On January 19, 1972, an official of the U.I.C. in Ottawa advised the Security Service that the information flow to the Security Service in "A" Division would be resumed. Two senior officers of the Security Service in "A" Division became the Security Service contacts with the U.I.C. (Exs. HC-1, pp. 5-6, 17, 28-30; HC-2, pp. 1-2).

35. This arrangement continued until the summer of 1973 when the Special Investigation Division (S.I.D.) of the U.I.C. made a new arrangement with the Security Service at Headquarters to create an information flow (Ex. HC-1, p. 32). The Security Service operated under this arrangement until June 12, 1978, and because of this new arrangement, "A" Division's relationship with the U.I.C. ceased (Vol. C16, p. 1940).

36. In addition to the Headquarters arrangement, working relationships existed between the local offices of the Security Service and the local offices of the U.I.C. These contacts were tolerated by the sources branch of the Security Service at Headquarters (Vol. C16, pp. 1949-50; Ex. HC-1, p. 61).

37. Finally, the evidence indicates that from October 30, 1973 until the fall of 1977 a quite distinct relationship existed between the Security Service at "O" Division in Toronto and employees of the U.I.C. offices there. The Security Service in Toronto could obtain information contained on social insurance application forms and then check it against the benefit records maintained by the U.I.C. on its National Claim Tape. The Security Service member could then contact the District Office of the U.I.C. to obtain further information (Vol. C16, pp. 1946, 1953, 1955-6; Ex. HC-1, pp. 52-53, 55, 62). With the disbanding of the S.I.D. at the U.I.C. in 1975, "O" Division's contact was directed to a contact at U.I.C. Headquarters in Ottawa. This direct contact ceased in the fall of 1977 (Vol. C16, pp. 1958-59, 1962).

38. There is one aspect of the correspondence between Ministers in 1971 which we wish to mention. At the request of Mr. Starnes, Mr. Goyer wrote to Mr. Mackasey, the Minister responsible for the U.I.C., requesting the co-operation of the U.I.C. On August 18, 1971, Mr. Mackasey replied to Mr. Goyer agreeing to the suggested meetings between the U.I.C. and the Security Service

> . . . to discuss this whole matter and to formulate a policy recommendation concerning all matters associated with the question, such as the Unemployment Insurance Act and Security Service requirements.

He also stated:

> . . . the provisions affecting the release of information from the Central Index of the Unemployment Insurance Commission have been modified somewhat under the new Unemployment Insurance Act. One of the pur-

poses, therefore, of the proposed meeting between the officials of our two Departments would be to review these new requirements in order to determine how the Commission can provide assistance to the R.C.M.P. within the framework of this new legislation.

(Ex. HC-2, p. 4.)

A meeting was held between representatives of the Security Service and the U.I.C. in October 1971 with the U.I.C. representative reported as stating he would have to discuss the matter "with others". On November 25, 1971, a memorandum written within the Security Service to the Security Service representative, as to what should be said in future discussions with the U.I.C. representative, stated:

> We suggest that in your discussions you subtly let him be aware of the fact that you know that *his Minister has agreed in principle to co-operate with the Force in this matter, without showing him the actual correspondence.*
>
> (Our emphasis added.)

Now, Mr. Mackasey's letter could not be read as "agreement in principle to co-operate with the Force in this matter" in the sense that he had agreed in any operative sense to provide information to the Force. One can readily infer that the reason for not showing the U.I.C. representative Mr. Mackasey's letter was that, without seeing it, the U.I.C. representative would more likely swallow the "subtly" communicated false information. Such an attitude by the R.C.M.P. toward another department of government is indefensible.

39. The only evidence as to whether, in 1972, the U.I.C. representative at the October meeting ever spoke to the Chairman of the U.I.C., is that of a member of the R.C.M.P. Indeed his evidence does not include any indication, even by hearsay, as to whether the U.I.C. official obtained any approval from anyone for the arrangement he entered into.

40. The association between the Security Service and U.I.C. was "never a point of concern from the point of view of legality" in so far as the Force was concerned (Vol. C16, p. 1966). Moreover, as far as was known by an officer of the Security Service who testified before us, the U.I.C. had not made it a "matter of legal concern". It is difficult to reconcile this position with a Security Service memorandum dated January 6, 1972, from a senior officer of the Security Service to the Deputy Director General, which recorded that at a meeting with a senior official of the U.I.C. the official had said that

> the matter could be raised verbally directly with the Chairman... who would decide whether or not it would have to be taken up with the Minister or whether an arrangement could be made for co-operation on a limited and sub rosa basis.

Anyone reading that memorandum's reference to co-operation on a "sub rosa basis" would be aware that there were problems.

Extent and prevalence

41. There is no evidence as to the extent to which information was provided by the U.I.C. to the Security Service at the divisional level of the R.C.M.P. However, the person at Headquarters who contacted the U.I.C. from the

summer of 1973 to September 1977, testified as to the extent to which Headquarters obtained, or attempted to obtain, information. In 1974 he made 127 requests, in 1975, 134 requests, in 1976 (the year of the Olympic Games in Montreal) he made 373 requests, and in 1977 567 requests. His successor made 136 requests from September 1977 to June 7, 1978. After June 12, 1978 no further requests were made (Vol. C16, pp. 1944-61, 1976).

Legal issues

42. The legal issues are identical to those discussed in connection with the C.I.B.

D. OTHER FEDERAL GOVERNMENT DEPARTMENTS AND AGENCIES

Department of National Health and Welfare: Family Allowances and Old Age Security

43. We did not inquire into whether the Security Service obtained access to family allowance and old age security information. We do know that, as in the case of access to information in the possession of other federal government departments, on July 27, 1971, Mr. Goyer, at the request of the R.C.M.P., wrote to the Minister of National Health and Welfare to request access to "the considerable biographical and other data on persons which is maintained in the Department of National Health and Welfare (Canada Pension Plan and Family Allowance and Old Age Security Divisions)", which he said "could be of great value to the Security Service in the discharge of its duties". The letter asked for interdepartmental discussions to determine "whether the requirements of the Security Service could be met within the framework of existing laws and regulations and in a manner which would attract no attention or criticism". In his reply of August 18, 1971, the Honourable John Munro, Minister of National Health and Welfare, wrote as follows:

> While I am sympathetic with the desire of the R.C.M.P. to reduce costs and improve efficiency in their operations, I am afraid that I would have to oppose in principle the use of data secured in connection with applications for Social Security benefits for any other reasons than to determine entitlement to those benefits.
>
> It has been our experience over the years in building up a structure of Social Security plans for Canadians that in order to secure the acceptance of the people of Canada of the various plans which have been introduced, one of the essentials is for them to have the assurance that the information they must provide will be kept in strict confidence, and will not be used for other purposes. This is reflected in the fact that in each of the laws which provides for the payment of social benefits there is a prohibition limiting our authority to disclose information obtained under the Act or the Regulations to situations where it is essential that this be done in order that the legislation may be properly administered.
>
> For any change to be made legislative action would be required, and I believe that even if we were not opposed in principle such amendments

> would not be acceptable to Canadians generally, particularly in the light of present conditions. As I indicated earlier, it is necessary for the people of Canada to accept the various laws if they are to be effective as approved by Parliament. There is no question in my mind, again apart altogether from the principle of the matter, that many persons, however much they might wish to receive certain benefits, would be reluctant to make application if they felt that the details they would have to provide concerning themselves and their families could be used against them in some other way.

(It may be noted that it was not strictly correct to say that "each of the laws" prohibits disclosure of information except "where it is essential that this be done in order that the legislation may be properly administered". For, as has been seen, the Old Age Security Act at the time already allowed information to be communicated to six other federal departments whose functions did not include administration of the Old Age Security Act.)

E. NEED AND RECOMMENDATIONS

44. In Part V, Chapter 4, we shall recommend that the security intelligence agency have access to the same federal government information as we propose for the R.C.M.P. in criminal investigations — that is, all personal information with the exception of census data collected and held by Statistics Canada. Our proposed system of controls to govern such access is similar to what we recommend for other highly intrusive investigatory methods. For personal information not merely of a biographical nature, the security intelligence agency would require the approval of the Solicitor General before making an application to a judge for a warrant.

CHAPTER 7

COUNTERING — SECURITY SERVICE

A. NATURE, ORIGIN AND PURPOSE OF DISRUPTIVE COUNTERING MEASURES

1. Some of the R.C.M.P. Security Service's practices which have involved activities not authorized or provided for by law have been referred to as 'countering activities'. There is considerable confusion as to what is included under countering activities. Some witnesses referred to the successful collection of intelligence about a security threat as a method of countering, but this usage is so elastic as to be meaningless. We prefer to limit the use of the word 'countering' to any positive steps that may be taken by the agency itself as a result of the collection and analysis of information, other than reporting intelligence to government. Some of these steps have traditionally been taken by other government departments or police forces rather than by the R.C.M.P. Security Service. Some of the measures taken by the Security Service have been unlawful. Of the lawful countermeasures, some have been of a nature that are appropriate to a security intelligence agency, while others in our view are not.

2. Some of the countermeasures undertaken by the Security Service have been regarded within the Service as 'disruptive', a phrase used to describe activities directed by the F.B.I. in the late 1960s against certain groups in the United States. A memorandum of June 11, 1971 (Ex. D-2), from the officer in charge of "G" Branch in Montreal, describes 'disruptive tactics' as follows:

> Making use of sophisticated and well researched plans built around existing situations such as, power struggles, love affairs, fraudulent use of funds, information on drug abuse, etc., to cause dissension and splintering of the separatist/terrorist groups.

Certainly this suggestion was at least partly inspired by belief that these tactics were in use in the United States, but since in a sense all countermeasures are 'disruptive' in their desired result, the word itself is unhelpful in assisting us to discriminate between acceptable and unacceptable countermeasures.

3. The use of tactics that, while not contrary to law, are intended to disrupt the effectiveness of a targetted organization, is not new. There is documentary evidence that the R.C.M.P., in 1956, distributed at least one letter among members of the Labour Progressive Party — a letter which was prepared by the R.C.M.P. as if it were written by a member of the Party and attacked the Soviet Union on a vital issue and the Soviet Communist Party's post-Stalin

leadership generally. The letter, which we saw, was reported to Commissioner Nicholson and Assistant Commissioner Harvison, both of whom had approved the operation, as having caused "definite concern and confusion within the Party ranks".

4. The national programme of 'disruptive' countermeasures from 1971 to 1974 under the code names ODDBALL and CHECKMATE, which is referred to in some detail later, was developed by a Special Operations Group at Headquarters. The officer in charge, who thereafter rose to a senior rank, stated in a memorandum in 1979 that

> (a) The use of calculated and measured security responses must be viewed in a historical perspective. Checkmate was developed and implemented as a proactive measure to contain or neutralize political violence at a time when such violence was rapidly increasing and accumulating. The lessons of the F.L.Q. crisis had indicated both to the government and to the Security Service that reactive or passive measures were not adequate. The government's invocation of the War Measures Act was a security response which it did not relish nor wish to use again. The onus to ensure this clearly fell within the mandate of the Security Service.
>
> (b) Checkmate was a calculated and measured security response aimed at containing or preventing the occurrence of political violence. It was strictly controlled to prevent abuses, but vigorously propagated to ensure results.
>
> (c) Many legal mechanisms in place at the time were either reactive and therefore inappropriate to intelligence needs, or were inadequate in terms of new security threats.

For these reasons he and the officers who served on the Special Operations Group consider that the countermeasures undertaken as part of this programme should be viewed against the background of the times. The reasons for the programme, as he described them in his testimony, can be summarized as follows:

(a) In the late 1960s the Security Service found itself faced by what it perceived to be an evolving threat to Canadian internal security which was different from the Communist threat which had been posed in the past. The new threat was seen as being a world-wide confrontation with authority by various groups employing violence for political ends.

(b) Violence erupted on the part of students and union members in France in 1968. Students battled police in the Federal Republic of Germany and Mexico. Mexican terrorists were recruited in Moscow and trained in North Korea. There was violence in the Middle East, and Palestinian violence began to spread elsewhere in the world. Palestinian terrorists began to work with the Japanese Red Army and the Baader-Meinhof gang. In 1972 the J.R.A. was responsible for a massacre at Lod Airport in Israel and the Baader-Meinhof gang supported the Palestinian Liberation Organization massacre at the Olympic Games in Munich. There was growing violence in South America. In the United States there were major confrontations, including acts of violence and bombings, by such groups as the Weather-

men and the Students for a Democratic Society. A strong and active black 'extremist' movement developed in the United States, including the formation of a Black Liberation Army, which was responsible for the killing of policemen in New York City.

(c) In Canada in the late 1960s and early 1970s there were growing numbers of confrontations and bombings, kidnappings and murder. The Security Service was concerned about what it saw as a growing black 'extremist' movement which was believed to have contacts with the black 'extremist' movement in the United States. Computers at Sir George Williams University were destroyed by students in 1969. The Security Service was also perturbed by small Marxist groups which it identified as New Left groups. These groups were considered to be responsible for demonstrations in which there were confrontations with the police. Some of these groups had contacts with groups in the United States. New Left activists from abroad, such as Daniel Cohn-Bendit and Jerry Rubin, visited Canada. The Security Service had a "major concern" that the New Left groups, the black 'extremists', the F.L.Q. "and the like" might form a common front. There was also an organization which was involved in 39 street confrontations and other incidents with the police, out of which arose 175 convictions. Palestinian activists visited Canada, contacted the F.L.Q., and provided guerrilla training to F.L.Q. members in the Middle East. Eight letter bombs addressed to Canada were intercepted outside Canada. The Security Service was also concerned with the Trotskyist movement which, at a World Congress in 1969, had approved the use of guerrilla warfare in South America. Canada and four other countries experienced the bombing of Yugoslav embassies and in Sweden the Yugoslav ambassador was murdered. Anti-Castro Cubans bombed Cuban mission premises in Ottawa and Montreal.

5. To meet some of these threats or perceived threats, Canadian police forces and the Department of National Defence were forming their own intelligence units. The police forces hoped thereby to develop evidence for the purpose of criminal prosecution. However, they found that prosecutions could rarely be launched or carried to a successful conclusion except when violent confrontation occurred on the streets. A feeling developed that, because the law could be applied only after offences were committed, the enforcement of the law was an inadequate means of effectively forestalling politically motivated acts of violence (Vol. 169, pp. 23254-5). Consequently, in 1970 the Security Service established the Special Operations Group, the purpose of which was to bring forward for the Countersubversion Branch innovative objectives and goals on a national basis. In 1971, this group acted upon what they understood to be the Director General's wish that there be more emphasis on containment, prevention and neutralization (Vol. 169, p. 23271). When discussing ODDBALL, an R.C.M.P. officer told the Group that they were to create programmes of disruptive measures where the target was of such a nature as to make such measures necessary. The limits were set first by the extent to which the operation was necessary, and second by the extent to which positive benefits could flow from the operation. There is no evidence before us of any consider-

ation having been given to whether operations should be within the law (Vol. 169, p. 23278). In June 1972, disruptive measures were authorized including "widespread harassment at every possible opportunity", against one Maoist group considered to be responsible for much violence. This was contemplated as consisting of the enforcement of by-laws and statutes, the execution of warrants, the initiation of deportation proceedings and the exploitation of rifts (Ex. PC-78, Tab 33). In March 1972, at a meeting of senior officers, Mr. Starnes urged that branches of the Security Service be "far more vigorous in their approach to disruptive activity" and promised his complete support for "well conceived operations". In a summary of the meeting, subsequently distributed by him, the "neutralization" of an organization or individual whose purposes were "clearly seen" to be "at cross-purposes with the maintenance of domestic stability" appeared as part of the discussion. Security Service officers in the field, said the memorandum, should not allow "reticence" to influence their work in disruptive operations, and if they failed to comply with tasks set for them by Headquarters, they "would be subject to censure, including, if necessary, transfer" (Ex. PC-78, Tab 26).

6. A senior member of the Special Operations Group considers that any CHECKMATE operations were proper "without any regard to whether they were... lawful or unlawful" as long as they were "responsible", "reasoned" and "measured". In his mind, any operations that met those criteria were as acceptable as a peace officer's interception of the driver of a speeding or recklessly speeding vehicle. He told us that in his basic training he was taught that the law permitted reasonable response when in other circumstances the same conduct would be illegal. He equated the emergency situation — the need to apprehend an offender who is committing an offence — with taking measures to bring an end to circumstances which, if unchecked, could lead to "the ascendency of violence" in Canada (Vol. 173, p. 23640).

7. If we may generalize from the case of this witness, an experienced member with a university degree, the early training of members of the R.C.M.P. as to what their powers are as peace officers appears to be significant. Such training had a bearing on the ability of members of the Security Service, in the early years of the past decade, to appreciate the limits of their authority. A peace officer undoubtedly has lawful power in an emergency, or when a crime is being committed or is about to be committed, to take reasonable steps to protect the lives of persons or to apprehend offenders. But this power ought not to be invoked by a well-trained policeman in other situations where the possibility of violence is general rather than immediate.

B. R.C.M.P. POLICIES AND PRACTICES

8. Security Service countermeasures were developed over the years sometimes on the initiative of Headquarters and sometimes as a result of local initiatives. Any countermeasures that could be called a 'programme' would require the support and even the initiative of Headquarters because of the need to commit resources of money and personnel to such activity. The current "policy", as stated on July 4, 1977, by the then Deputy Director General (Operations),

Assistant Commissioner Sexsmith, requires all countermeasures operations to be approved by the Deputy Director General (Operations) and to be "conducted within the limits of lawful authority and by legal means". However, there is evidence that the requirement of approval by the Deputy Director General (Ops) is not regarded as more than a general rule, and that countermeasures approved by the officer in charge of a 'desk' or section at Headquarters will not be regarded as unauthorized.

9. Within the R.C.M.P., both in the Security Service and in senior ranks of the R.C.M.P. generally, many forms of countermeasures have been well-known for decades. Perfectly proper methods of countering include: encouraging foreign intelligence officers to become double agents or to defect; briefings of government departmental officials or travellers as to the dangers of compromise; lawful arrest and prosecution. At the other extreme are disruptive tactics that include an element of unlawfulness, such as some of the CHECKMATE operations. While it is true that in the early 1970s the R.C.M.P. was urged to be "pro-active" — a word that appears to have been invented to describe action before the event rather than afterward — that word carries no connotation of illegality or indeed of anything more than the vigorous collection of intelligence before a crisis develops. Between these acceptable and unacceptable extremes are countermeasures that, while lawful in concept and execution, are in our view inappropriate functions of a security intelligence agency. Some examples of such countermeasures are inducing employers to discharge subversive employees, or leaking information to the media about the subversive characteristics of individuals, or undertaking "conspicuous surveillance" of domestic groups or attempting to prevent one group from subverting another political party.

C. EXTENT AND PREVALENCE OF COUNTERING MEASURES

10. Our analysis of 'extent and prevalence' applies not only to those countering measures that might be said to be "not authorized or provided for by law", but also to activities which, although they may have been lawful, are not acceptable. We analyze two categories of countermeasures — those carried out by some members of "G" Section of the Security Service, concerned with terrorism in Quebec, working in and outside Montreal in the early 1970s, and those carried out by members of the Security Service in several other provinces in the years 1971 to 1974 under the umbrella code names of ODDBALL and CHECKMATE.

11. The activities in Quebec included the following:

(a) The burning of a barn in which a meeting of a group believed to be subversive was to have been held. The evidence before us is that the object of the operation was to cause the group to move to another location where electronic surveillance would be feasible. However we cannot dispel from our minds the possibility that the members of the Security Service who participated in that incident also contemplated that the result would be a 'disruption' of the group's activities. There is no evidence to indicate that there was any other incident involving similar destruction of private property other than documents.

(b) Attempts in 1971 and 1972 to recruit human sources in groups believed to be violence-prone. To some extent disruption was the rationale behind the attempts. If in a particular case the attempt to recruit were to be successful, the result would be receipt of information about the activities of the group; if the attempt were unsuccessful, the attempt itself might become known to other members of the group who might then regard the target of the attempt with suspicion. Thus the very attempt might produce factionalism and disruption.

(c) Issuing a communiqué with the intention that the news media and members of the F.L.Q. and their sympathisers would regard it as a legitimate call to arms. There is no evidence that such a document was produced more than once by the R.C.M.P.

(d) Attempting to disrupt, by conspicuous surveillance, a meeting of members of an activist cell held in rural Quebec in September 1978.

12. The activities in other provinces, under the code names ODDBALL or CHECKMATE, were developed by a Special Operations Group at Headquarters. Members of the Security Service across Canada were encouraged to propose plans for new methods to help deal with threats of violence and of activities by political groups and organizations considered to be agents of hostile foreign powers. The evidence of those operations that were carried out included several that involved activities that might be characterized as "not authorized or provided for by law" in the sense that criminal acts may have been committed (attempting to render a vehicle inoperative, filing an income tax return in the name of another person, theft of a letter, and threats by phone). There was also one operation in which a criminal act (assault) was under consideration but not carried out. In our investigation of the nature, extent and prevalence, of these operations, the destruction of CHECKMATE files has made us entirely dependent on a few members of the Security Service, who have reconstructed what occurred from memory.

13. In addition, the following incidents have occurred. They may not have been unlawful in the circumstances, but represented activities the acceptability of which is a matter of policy. They will be discussed in Part V, Chapter 6. Some of these incidents occurred under Operation CHECKMATE; others did not:

(a) An approach to the employer of a person regarded as a terrorist or a supporter of a terrorist or a 'subversive' group with a view to persuading the employer to discharge the person. One incident is known.

(b) Dissemination of adverse information through the media, believed to be true, about an individual or group regarded by the Security Service as a security threat. Two incidents are known.

(c) Spreading information, believed to be true, designed to discredit the leader or other members of political or other organizations or to create dissension among 'subversive' groups. Two occasions are known.

(d) Spreading information, known to be false, designed to discredit a leader of an organization regarded as 'subversive'. One incident is known.

(e) Communicating anonymously with leaders of a political party to warn them that some members of their party were planning to attempt to obtain

delegates' credentials for the leadership convention of another political party in the hope of influencing the outcome of the convention. One instance is known.

D. LEGAL AND POLICY ISSUES

14. The present mandate of the Security Service authorizes it to "deter, prevent and counter" certain specified activities. Within the Security Service there has been no suggestion that these verbs should be assigned different meanings, and we can see no advantage in seeking to do so. Nor did the formal submission to the Cabinet in March 1975 discuss the meaning or consequences of these verbs.

15. Mr. Starnes and Mr. Dare consider that the use of these words in the Cabinet Directive of March, 1975, was in effect a declaration of already existing functions of the Security Service. Thus Mr. Starnes, both when he was Director General and when he testified before us on this subject in 1979, considered it natural that the Security Service should undertake a programme of countermeasures; he considered that the 'countering' work of a security intelligence agency is implied by the very use of the terms 'counter-espionage' and 'counter-subversion'.

16. Thus may words become masters. Whether or not the professional terminology authorized 'countering', two real questions remain: was, and is, 'countering' a proper and acceptable function of a security intelligence agency? If it is, what kinds of 'countering' are permissible and subject to what controls?

17. Some activities that may be characterized as "countering" are an inevitable and proper result of the work of such an agency. The collection of information, and its assessment and transformation into intelligence, may be said to be part of the countering process, in the sense that without collection and assessment nothing can be done, although to describe collection and assessment as countering is to expand the definition of the term beyond its real limits. A more obvious countering activity involves the 'turning' of a member of a hostile intelligence agency so that, while pretending to be still a genuine agent of that agency, he in fact provides information to the Canadian security intelligence agency. He becomes a double agent. If the Canadian agency can obtain such information about the activities of the hostile agency's espionage in Canada, those activities can be neutralized effectively. Thus the development of an 'agent in place' has 'countering' consequences, but it is unhelpful to describe this technique as a method of 'countering'. In reality it is providing a source of information that may also be used as a vehicle for a countering operation. It is not only legitimate but desirable for a security intelligence agency to be successful in persuading members of hostile foreign agencies to defect so that the Canadian agency and its allies will have an improved knowledge and understanding of the structure, personnel and methods of the foreign agency.

18. Information collected by the security intelligence agency is often transmitted to police forces and government departments, and may prompt these

authorities to take preventive measures against individuals or groups. For instance, security intelligence about terrorists is given to the police who are responsible for protecting international visitors, and intelligence about terrorist or espionage agents may be given to a police force having jurisdiction to investigate crime so that it can be used as evidence. Information about the secret intelligence activity of a foreign diplomat might be given to the Department of External Affairs so that the Secretary of State for External Affairs may decide whether to declare that diplomat to be *persona non grata* or otherwise let it be known to the foreign country that his activities are unacceptable. Similarly, in the security screening process, reports from the security intelligence agency will affect decisions by government departments to deny security clearance. The security intelligence agency may also pass information directly to individuals in preventive security briefings. For instance, the agency may warn Canadians posted abroad or intending to travel in certain countries of the methods which may be used to induce them to become sources for a foreign agency. In all of the foregoing situations, the preventing or countering action is taken by a police force or government department exercising an authorized governmental function, and the security intelligence agency's contribution is confined to its proper role of collecting and reporting security intelligence.

19. In the past, the "deterring preventing and countering" role of the R.C.M.P. Security Service went far beyond the proper functions of a security intelligence agency. Countering activities that are not acceptable include any that are contrary to the law of Canada, whether it is a federal, provincial or municipal law or the common law or the Quebec Civil Code. The legal issues arising from any of the incidents mentioned earlier which may have involved acts "not authorized or provided for by law" are analyzed in a separate Report. As we have noted, the legality of Security Service countermeasures was not a consideration for R.C.M.P. officers. This disregard for the rule of law is completely unacceptable under the system which, later in this Report, we shall propose for the future. No countermeasure should have been permitted which violated any Canadian law. No unlawful countermeasures by the security intelligence agency should be permitted in the future. Nor do we see any need to recommend changes in the law which would make otherwise unlawful countering measures lawful.

20. There are also countermeasures designed to disrupt the activities of groups or of individuals regarded as subversive which, while not unlawful, are nevertheless objectionable and unacceptable. This is particularly the case when the individuals concerned are Canadians employed in purely domestic political activities and not acting as foreign agents. We find it entirely inappropriate for the Canadian state, through an agency the operations of which are essentially secret, to take coercive measures against Canadian citizens and put them at a serious disadvantage. Later in this Report, in Part V, when we set out our recommendations on the laws and policies which should govern the Government of Canada's security intelligence activities, we shall discuss in detail the kinds of countering activity which must be avoided in the future as well as those which are acceptable.

21. The Security Service's use of unlawful countermeasures and those unacceptable measures referred to in the last paragraph was a grave mistake. These methods violated the rule of law, inflicted damage on Canadian citizens and involved secret attempts to manipulate political events and the news media. Such practices not only violate important precepts of Canadian democracy but they may also seriously damage the security agency itself. First there is the corrupting effect which the carrying out of such 'dirty tricks' is likely to have on the ethos of the security intelligence organization. Secondly, there is the loss of public respect which the disclosure of such tactics is likely to engender. Approval of such tactics will reduce the public's support for any kind of secret security intelligence activities.

CHAPTER 8

PHYSICAL SURVEILLANCE

A. ORIGIN, NATURE AND PURPOSE OF THE PRACTICE

1. When it is used in the course of R.C.M.P. investigations, the term "physical surveillance" includes the following practices:

(a) the use of static or mobile facilities to observe activities occurring in and around a fixed target such as a building;

(b) the use of cars, motorcycles, airplanes or boats to follow a target;

(c) the deployment of persons on foot to follow and watch a target; and,

(d) the use of technical aids to surveillance.

While the purpose of physical surveillance has remained unchanged, techniques have grown more complex over the years to cope with increasingly sophisticated methods of transportation and counter-surveillance. In the Security Service, physical surveillance is used to monitor the clandestine activities of intelligence agents from hostile countries, domestic groups which pose a threat to Canada's security, and agents of international terrorism. This surveillance enables the Security Service to acquaint itself with the personal habits of the human targets, follow their movements, and learn of any clandestine relationships they may be cultivating in this country.

2. Physical surveillance operations on the criminal side, unlike those in the Security Service, are usually aimed at obtaining information which will result in a criminal prosecution. It is for this reason that C.I.B. surveillance operations are generally of shorter duration than their Security Service counterparts. Physical surveillance by the C.I.B. is frequently directed at drug crimes and organized criminal activities.

3. Because of their different organization and objectives, it is convenient to deal separately with the structure of the Security Service and C.I.B. surveillance units.

The Security Service

4. One branch of the Security Service is responsible for visual monitoring on behalf of all the main operational branches of the Service. It is basically a technical service unit called in to provide visual surveillance of targets in counter-espionage or counter-subversion operations, and is often referred to as the "Watcher Service". Although its responsibilities were later expanded to

provide surveillance support for all Security Service activities, initially it was created to satisfy the surveillance needs of the Counter-espionage Branch and in fact was first a section of that Branch.

5. The creation of the Watcher Service was inspired by considerable clandestine espionage activity on the part of Communist bloc intelligence services, a significant portion of which was going undetected. A greater commitment to physical surveillance was intended to uncover that activity. The part-time surveillance effort in use until 1954 was incapable of meeting the challenge posed by increased foreign activity in Canada. The Security Service committed itself to the creation of a surveillance operation intended to possess a high level of skill and continuity of experience. In essence, the Security Service sought to specialize.

6. Surveillance, when required, may also be handled by regular members, most of whom have received training from Watcher Service members, as have many C.I.B. members and officers from other police forces.

The Criminal Investigation Branch (C.I.B.)

7. Before the early 1970s, surveillance of a criminal target was carried out according to manpower and equipment availability, without central co-ordination by a particular branch. No specialized group capable of conducting intensive coverage existed. Results of surveillance were haphazard. In the early 1970s, investigators at Montreal's "C" Division were conducting wide-ranging surveillance of targets. Because these targets routinely employed counter-surveillance methods, a need was recognized for a specialized surveillance unit, capable of maintaining surveillance on difficult targets. This gave rise to the first specialized C.I.B. surveillance team, which responded to requests for surveillance on targets of interest to various C.I.B. sections at "C" Division. Subsequently, specialized surveillance teams were introduced to several other divisions.

8. In March 1973 the R.C.M.P. designated the National Crime Intelligence Branch (N.C.I.B.) to co-ordinate policy and supervise the activity of surveillance sections in C.I.B. divisions throughout Canada. In July 1974 the N.C.I.B. surveillance sections were renamed Special "O" Sections. Terms of reference now govern the duties and operational procedures for Special "O" Sections. The duties include the collection of strategic and tactical criminal intelligence on predetermined targets, familiarization through surveillance with the habits and descriptions of regional organized crime figures, obtaining photographs of suspect individuals, buildings and meetings, and reporting random sightings of organized crime figures. In addition, surveillance assistance is given to all R.C.M.P. investigative squads and other Division Criminal Intelligence Service (D.C.I.S.) sections. Special "O" Sections are comprised of regular members, who fill most of the supervisory positions, and Special Constables who comprise the surveillance teams. Special Constables are given preparatory training for eight weeks. As in the Security Service, C.I.B. surveillance units have been forced to employ increasingly sophisticated techniques as targets themselves become more adept at detecting and countering surveillance.

B. LEGAL ISSUES

9. There are three categories of statutes which have presented difficulties for surveillance work:

— those governing "rules of the road";

— those governing the identification of persons and property; and

— those relating to trespass.

Rules of the road

10. The movement of motor vehicles on the highway is primarily regulated by provincial statute. Representations made to us indicate that adhering to these rules of the road when engaging in intensive surveillance operations has not always been possible. Indeed, Watcher Service training has emphasized that "there is no place for timidity in surveillance work". One result of this lack of timidity has been the violation of provincial traffic laws — particularly when a vehicle carrying the target might itself not comply with traffic laws. In addition to the violation of provincial laws, surveillance team members may have breached municipal by-laws by committing "non-moving" violations.

11. We have examined instances where surveillance was unsuccessful because traffic laws were obeyed and we are satisfied that compliance with present traffic laws must in many cases be responsible for the loss of surveillance and a consequent loss of effectiveness of the security operation.

12. The following provincial traffic violations have been specifically brought to our attention: speeding, proceeding the wrong way in one-way traffic, illegal U-turns and failure to stop. The list of possible violations includes:

— unnecessarily slow driving

— failure to yield right of way

— improper turns or signals

— failure to obey traffic lights

— failure to drive in proper lane

— improperly overtaking other vehicles

— following too closely

— failure to yield for emergency vehicles

— failure to stop at railway signals

— failure to obey instructions posted on traffic signs.

Municipal "non-moving" violations have also occurred when surveillance drivers have stopped in a no-stopping or loading zone in order to maintain observation of a target.

13. The Criminal Code also creates offences in relation to the operation of motor vehicles on the roadway. Section 233(4) affords an example:

> (4) Every one who drives a motor vehicle on a street, road, highway or other public place in a manner that is dangerous to the public, having regard to all the circumstances including the nature, condition and use of

such place and the amount of traffic that at the time is or might reasonably be expected to be on such place, is guilty of

(a) an indictable offence and is liable to imprisonment for two years, or

(b) an offence punishable on summary conviction.

There has been no evidence before us to suggest that Criminal Code offences (such as criminal negligence and dangerous driving) relating to the operation of motor vehicles have been committed by those engaged in physical surveillance in order for them to carry out their duties. Nor has there been any suggestion that any authority to drive in such a manner is necessary in the future.

The most recent attempt by the R.C.M.P. to state policy in regard to traffic laws

14. A "bulletin" from the Commissioner of the R.C.M.P., Bulletin OM-82, sent to all members of the Force (both C.I.B. and the Security Service) on August 25, 1980, states:

> Every member of the R.C.M.P. discharging covert surveillance responsibilities, or overtly responding to emergencies is expected to comply with all relevant provincial statutes, regulations and municipal by-laws.

The bulletin then promulgates "guidelines" to apply in "exceptional" circumstances, where "total" or "strict" compliance with "provincial statutes, regulations and municipal by-laws relating to traffic control" may, "because of the nature and seriousness of an investigation", not be "necessary in the public interest".

15. The guidelines are as follows:

> (i) Legal authorities and various provincial and federal statutory enactments provide certain legal protection to members of the R.C.M.P. when acting reasonably and responsibly in the discharge of those duties they are empowered to perform.
>
> (ii) Notwithstanding that certain legal protection would be provided to members of the R.C.M.P. reasonably conducting their surveillance and pursuit duties, every member is expected to comply with provincial and municipal motor traffic requirements unless:
>
> — to do so would seriously inhibit and prevent surveillance and/or pursuit activity; and
>
> — there are exceptional circumstances; and
>
> — when;
>
> A. There are reasonable and probable grounds to believe,
>
> (1) Life is in danger;
>
> (2) An indictable offence is in progress;
>
> (3) An indictable offence is about to be committed;
>
> (4) An indictable offence has been committed, is under active investigation, and the surveillance and/or pursuit is essential for purposes

of either identifying those responsible for that specific offence, or collecting evidence deemed necessary for prosecution, or

B. The surveillance or pursuit is in regard to:

(1) Persons known to be currently active in major criminal activity, when it becomes apparent that crimes are being planned, the exact nature and extent of which are still undetermined.

(2) A V.I.P. visit where it is necessary to keep surveillance on or to pursue persons who might cause harm or serious disruption, and the surveillance or pursuit is taking place during the course of that visit, not in preparation therefor.

(3) The protection of Government property, as in the case of maintaining discreet surveillance on the carrier of a flash roll during undercover operations.

(4) Investigations with respect to subversive activity as defined in the Official Secrets Act.

Thus the Commissioner has told members engaged in surveillance duties that, apart from cases where the law *might* afford a defence (such as the defence of necessity) to a charge — for instance of going through a red light or speeding — members may ignore such laws if the conditions in the guidelines are all satisfied.

16. The "bulletin" is stated on its face to be part of the Operational Manual of the Force and the Commissioner has confirmed to us that it forms part of that Manual. The bulletin states that "The following general guidelines *must* therefore be adhered to in the future". (Our emphasis.) If those words constitute an "instruction or order", then failure to comply with them would be a breach of the Commissioner's Standing Order I.4.C.1.a. which reads:

> The conduct and activities of a member shall at all times be such as to bring credit to himself and to the Force. A member shall not:
>
> Contravene or fail to comply with any oral or written instruction or order issued in a manner authorized by the Commissioner.

Breach of such a standing order is a minor service offence under section 25 of the R.C.M.P. Act. However, the Commissioner has advised us that, notwithstanding his use of the imperative word "must" in the bulletin, he did not intend the bulletin to be an "order". He says it is "only a guideline". In our opinion it would be difficult for a member receiving the bulletin to know the legal nature of it. At the very least the member would be likely to regard the bulletin as advice from the Commissioner that conduct which, in the case of an ordinary citizen or even a policeman "cruising" in a patrol car would be a violation of provincial or municipal traffic laws, will be permitted by the Force in the sense that no disciplinary action will result if a member engages in the same conduct in the circumstances described in the bulletin. The Commissioner has told us that what he intended to convey by the bulletin may be summarized as follows:

(a) as a general principle every member of the R.C.M.P. engaged in surveillance activities is expected to comply with all provincial statutes and regulations and municipal bylaws;

(b) where certain conditions are met, activities which otherwise would be violations of those statutes, regulations or bylaws do not constitute such violations;

(c) the reference to "legal authorities and various provincial and federal statutory enactments..." providing legal protection to members is to such matters as the protection afforded by section 25 of the Criminal Code, section 26 of the Interpretation Act, defences such as that contained in the New Brunswick Police Act and common law defences such as necessity or the immunity alleged to exist for members of the R.C.M.P. as agents of the Crown;

(d) in essence, the bulletin sets out circumstances in which, according to the R.C.M.P.'s interpretation of various statutory and common law defences and immunities, no violations of provincial laws and regulations or municipal bylaws occur.

In promulgating this bulletin the Commissioner relied in part on legal advice obtained from the Department of Justice. In Part IV we discuss the various "defences", such as the common law defence of necessity, the "implied powers" provision of section 26.2 of the Interpretation Act, the "justification" principle embodied in section 25.1 of the Criminal Code, and the various doctrines of immunity, and we intend in the ensuing paragraphs to review each of these briefly in the present context. In addition, as far as New Brunswick is concerned, there is a provincial statutory defence to provincial offences; this defence is referred to by us in Part V, Chapter 4. In the following brief comments which we make with respect to the Commissioner's bulletin, what we say is fully applicable only to those provinces which do not have a statutory defence, i.e. all provinces other than New Brunswick.

17. The common law defence of necessity would be available in regard to provincial offences.[1] It would likely be available if life is in danger, or if an indictable offence is in progress or is about to be committed or has been committed and there is "hot pursuit" of the culprit, but even then it would be necessary to balance the competing interests identified in *Morgentaler* v. *The Queen*, which we discuss in Part IV. Focussing our attention on the specific situations referred to in Bulletin OM-82, we do not think that the defence of necessity would be available if "an indictable offence is in progress, or is about to be committed or has been committed and the surveillance or pursuit of the culprit is essential for the purposes of either identifying those responsible for that specific offence or collecting evidence deemed necessary for prosecution". For example, a member driving a police vehicle while engaged in attempting to identify a thief or a person who has wilfully damaged property, or attempting to collect evidence of such offences, would not be able to rely on the defence of necessity if he were charged with speeding or failing to stop at a stop sign or a

[1] As a matter of principle, the common law defence of necessity would be available for provincial offences, at least to the same extent as in prosecutions under the Criminal Code. See *R.* v. *Walker* (1979) 48 C.C.C. (2d) 126 at 144 (Ont. Co. Ct.). In Ontario now the provision found in section 7(3) of the Criminal Code, which preserves common law defences, is copied in respect to provincial offences: the Provincial Offences Act, 1979, ch. 4, section 80.

red light. Similarly, we do not believe that the defence of necessity would be available where traffic violations are committed by a member conducting surveillance of those planning indictable offences, suspected of intending harm to visiting V.I.P.s, or plotting damage to government property. The sense of proportion between the perceived harm in the conduct of the criminal and the departure from regulated conduct on the part of the member — so essential to the application of the defence — cannot be assumed in advance as the Bulletin seems to do.

18. In Part IV we also discuss section 26(2) of the Interpretation Act and express the opinion that it cannot be invoked as authority in support of an implied power to do that which otherwise would be unlawful. We also discuss section 25(1) of the Code and, citing *Eccles* v. *Bourque*, conclude that it provides justification for a peace officer only for the use of "force" and then only when the law requires or authorizes him to do the very thing in question; violating a traffic law would probably fail to satisfy either condition in a number of the circumstances specifically referred to in the Bulletin.

19. It is apparent from what we have learned that the Commissioner's Bulletin is also founded on advice that provincial law is not applicable to actions of members of the R.C.M.P. that are "reasonably necessary to enable them in particular circumstances to carry out duties and responsibilities assigned to them by or under federal legislation". This opinion is founded on the statement by Mr. Justice Pigeon, delivering the reasons for judgment of the Supreme Court of Canada in the *Keable* case,[2] that the R.C.M.P. is a branch of the Department of the Solicitor General and its management as part of the Government of Canada is unquestioned. The advice given to the R.C.M.P. appears to be an invocation of certain of the doctrines of immunity which we discuss fully in Part IV. We consider that, in its stated breadth of application, it is likely not an accurate statement of the law, and that it may be an invalid foundation for the Commissioner's Bulletin. We emphasize that we do not criticize Commissioner Simmonds, who is entitled to rely on such advice, especially when it comes from the source from which it did come. Consequently, we have serious doubts as to the legal foundation of Bulletin OM-82. We realize that it is not easy to frame guidelines for members concerning these matters, in the light of the present state of the law. Implementation of our recommendations would result in both the R.C.M.P. and the security intelligence agency having less difficulty in instructing their members in the future. In the meantime, for the reasons we shall give in Part IV, we do not think that members of the R.C.M.P. should rely on Bulletin OM-82 as authority which could be cited as a defence if they are faced with charges under provincial or municipal traffic laws, except in those circumstances when the defence of necessity would properly apply.

Laws governing the identification of persons and property

20. A number of federal and provincial statutes require the accurate identification of persons or property. Examples include various provincial enactments

[2] *Attorney General of Canada* v. *Keable* [1979] 1 S.C.R. 218 at 242.

requiring hotel guests to register in their proper names, and highway traffic legislation requiring individuals to hold a valid driver's licence and identify their automobiles with provincially issued licence plates.

21. Registration and identification requirements are incompatible with the covert nature of surveillance operations. As in the case of undercover operations involving members or human sources, the ability to conceal one's true identity successfully is essential in physical surveillance operations. A target, once aware of a surveillance effort, may simply delay his intended clandestine or criminal activity, or deliberately mislead the surveillance team. Furthermore, the team, once "burned" (exposed to a target) is of little value in further covert surveillance of that target. Hence, the need has arisen for surveillance cars to have licence plates that cannot be traced to the R.C.M.P., and for members to hold identification documents that allow them to remain in proximity to a target without disclosing their true identity.

22. At present, the two most commonly used false identification documents are drivers licences and vehicle registrations. This documentation has in the past been obtained in a number of ways: applying for the document in the normal manner, but supplying false information in the application; entering into agreements with senior departmental officials for the issuance of documents and, manufacturing high quality false documentation by the R.C.M.P.

23. Supplying a false statement in an application for a driver's licence (in order to obtain a licence in a false name) is an offence in most provinces, as is the possession or use of a fictitious licence. Further violations occur in some provinces where an individual holds more than one valid licence or applies for a second licence while holding a valid licence. Finally, a licence may be invalid in some provinces unless signed in the "usual signature" of the individual licenced.

24. Dual registration of a surveillance vehicle violates other Highway Traffic Act provisions in a number of provinces. Over the years a variety of practices have been used to disguise the ownership of R.C.M.P. surveillance vehicles. It is impossible to outline every variation of this practice; a few examples, however, are illustrative. In some cases, a car owned by the R.C.M.P. was registered in the name of an "ostensible owner", who may have falsely indicated in an application for registration that he was the true owner. In other cases, an additional set of plates may have been obtained through making an application, with the co-operation of provincial Registrars of Motor Vehicles, for vehicles already registered in the name of the R.C.M.P. It is an offence under provincial Highway Traffic legislation to make false statements (e.g. as to the applicant's true identity, or the ownership of a vehicle) in an application for registration; it is also an offence in some provinces to use licence plates other than those registered or issued for a vehicle. Finally, the use of out-of-province licence plates after a defined period of time may violate Highway Traffic legislation.

25. Where a licence or registration has been obtained through making a false statement in an application, such a statement may amount to a false pretence

under section 320 of the Criminal Code. Section 319 defines a false pretence as follows:

> (1) A false pretence is a representation of a matter of fact either present or past, made by words or otherwise, that is known by the person who makes it to be false and that is made with a fraudulent intent to induce the person to whom it is made to act upon it.

26. Section 320 states:

> (1) Every one commits an offence who
>
> (a) by a false pretence, whether directly or through the medium of a contract obtained by a false pretence, obtains anything in respect of which the offence of theft may be committed or causes it to be delivered to another person;
>
> (2) Every one who commits an offence under paragraph (1)(a)
>
> (a) is guilty of an indictable offence and is liable to imprisonment for ten years, where the property obtained is a testamentary instrument or where the value of what is obtained exceeds two hundred dollars; or
>
> (b) is guilty
>
> (i) of an indictable offence and is liable to imprisonment for two years, or
>
> (ii) of an offence punishable on summary conviction,
>
> where the value of what is obtained does not exceed two hundred dollars.

On some occasions false registration and identification documents have been manufactured by the R.C.M.P. for use by the Criminal Investigations Branch in lieu of having members apply for licences and other forms of documentation. The manufacture of these documents may have amounted to forgery under section 324 of the Criminal Code. That section reads, in part:

> 324. (1) Every one commits forgery who makes a false document, knowing it to be false, with intent
>
> (a) that it should in any way be used or acted upon as genuine, to the prejudice of any one whether within Canada or not, or
>
> (b) that some person should be induced, by the belief that it is genuine, to do or to refrain from doing anything, whether within Canada or not.
>
> (3) Forgery is complete as soon as a document is made with the knowledge and intent referred to in subsection (1), notwithstanding that the person who makes it does not intend that any particular person should use or act upon it as genuine or be induced, by the belief that it is genuine, to do or refrain from doing anything.
>
> (4) Forgery is complete notwithstanding that the false document is incomplete or does not purport to be a document that is binding in law, if it is such as to indicate that it was intended to be acted upon as genuine.

27. Section 326 of the Code creates an offence when the forged document is used:

> 326. (1) Every one who, knowing that a document is forged,
>
> (a) uses, deals with, or acts upon it, or

(b) causes or attempts to cause any person to use, deal with, or act upon it,

as if the document were genuine, is guilty of an indictable offence and is liable to imprisonment for fourteen years.

28. When a member engaged in surveillance assumes the identity of a person, whether living or dead, he may violate section 361 of the Criminal Code. That section reads:

> Every one who fraudulently personates any person, living or dead,
>
> (a) with intent to gain advantage for himself or another person,
>
> . . . or
>
> (c) with intent to cause disadvantage to the person whom he personates or another person,
>
> is guilty of an indictable offence and is liable to imprisonment for fourteen years.

In most surveillance operations there is no personation of a person "living or dead", so that no offence is committed. Where, however, an individual engaged in surveillance might purport (although we have seen no examples) to be another person, living or dead, he may violate the section.

29. In order for the offence to occur, the personation must also be fraudulent and the personator must intend to gain advantage for himself or cause disadvantage to the person he personates or another person. The word "advantage" in section 361 has been afforded a broad interpretation. In *Rozon* v. *The Queen*[3] Mr. Justice Montgomery stated:

> The words "gain advantage" could scarcely be more general in their scope, and I find nothing to suggest that their application should be restricted to an advantage appreciable in money.[4]

Mr. Justice Crête held that the word "advantage" must be taken in its larger meaning. [Our translation]

> In reading this text, one can see that the legislator has declared guilty of an indictable offence anyone who personates someone (a) to gain advantage — without specifying its nature; (b) to obtain any property or an interest in a property — this is specific, in view of the definition of the word "property" given in section 2 of the Criminal Code; (c) to cause disadvantage to another person — here again, without specifying the nature of the disadvantage.[5] [Our translation]

This reasoning was accepted in Ontario in *Regina* v. *Marsh*.[6] Thus it appears that almost any advantage or disadvantage is encompassed by section 361. Nonetheless, it may still be questioned whether the courts, in construing "advantage" so broadly, intended it to encompass the *investigative* advantage gained through personating another individual.

---

[3] (1974), 28 C.R.N.S. 232 (Quebec C.A.).

[4] *Ibid.*, at p. 233.

[5] *Ibid.*, at p. 237.

[6] (1975) 31 C.R.N.S. 232 (Ont. Co. Ct.).

30. The most significant restriction in section 361 is the requirement that the personation be "fraudulent". In *Rozon* v. *The Queen*, Mr. Justice Crête adopted a narrow construction of the word:

> In my opinion, the word fraudulently as used in section 361 is an adverb of manner which involves bad faith as opposed to good faith, or to an honest error.[7] [Our translation]

It therefore appears that an individual engaged in surveillance who personates another person, living or dead, and gains an advantage or causes a disadvantage thereby within the meaning of section 361, nonetheless commits no offence as long as he does not act in bad faith. The section then appears likely to be of no consequence in relation to surveillance operations which are carried out in good faith, i.e. for purposes falling within the mandate of the Security Service or the policing duties of the C.I.B.

31. The interpretation of section 362 of the Criminal Code, however, is problematical. That section, dealing with personation at an examination, reads as follows:

> 362. Every one who falsely, with intent to gain advantage for himself or some other person, personates a candidate at a competitive or qualifying examination held under the authority of law or in connection with a university, college or school or who knowingly avails himself of the results of such personation is guilty of an offence punishable on summary conviction.

We are aware of at least one instance, although not a surveillance operation, where this section may have been violated. As we have seen in our examination of section 361, the word "fraudulently" in that section implies bad faith on the part of the personator; the word "falsely" in section 362 may be interpreted in a similar fashion, thus absolving a personator acting in good faith (e.g. in order to carry out the mandate of the Security Service). The little case law which has construed the word "falsely" seems to support this interpretation. In *Rex* v. *Frank*,[8] Chief Justice Campbell of Prince Edward Island found that the offence of making a false statement in the Income War Tax Act, R.S.C. 1927, involved not merely an inaccurate statement, but one made fraudulently, with *mens rea* or intent to deceive. A number of American cases have reached similar conclusions.[9] Yet, "falsely" in section 362 is not so clearly defined that we can ignore the possibility that Security Service activities of the nature mentioned here violate the section. The example we have cited is not the only activity of this nature of questionable legality: individuals engaged in surveillance operations might also have violated section 362 if they chose to obtain their "cover" licences by supplying the name of a real person when taking their qualifying tests. We are not aware of any specific instances where individuals engaged in surveillance have personated other individuals in a manner that violates section 362; that does not mean, however, that the practice has not occurred. In any

---

[7] (1974) 28 C.R.N.S. 232 at p. 238 (Quebec C.A.).

[8] (1945) 84 C.C.C. 94 (P.E.I.S.C.).

[9] *U.S.* v. *Achtner*, 144 F. 2d 49 (C.C.A.N.Y.); *Fouts* v. *State*, 149 N.E. 551; *U.S.* v. *King*, 26 Fed. Cas. 787; *U.S.* v. *Otey* 31 F. 68.

event, this brief discussion serves to highlight the potential for running afoul of these sections as the R.C.M.P. search for new and legal means of obtaining "cover" documentation.

32. Disguising one's proper identity may also have resulted in violation of provincial hotel registration legislation. A number of provinces have legislation prohibiting hotel guests from registering in an assumed name or falsely stating their place of residence. This problem has been identified in four provinces in particular — Nova Scotia, Prince Edward Island, Ontario and British Columbia.

Laws relating to trespass

33. The surveillance sections of the Security Service and the C.I.B. have both indicated to us that violations of petty trespass legislation are inherent in surveillance operations. Common examples include entering parking garages in apartment buildings to determine the presence of a target's vehicle and entering an apartment building in order to determine by listening from a corridor whether the target is within an apartment. These activities may, depending on the circumstances, constitute a trespass to property in provinces having trespass legislation.[10] In addition, they may give rise to the Criminal Code offences of Mischief and Trespassing at Night.

34. Nova Scotia, Prince Edward Island and Saskatchewan have no trespass legislation. Trespass legislation in British Columbia and New Brunswick applies to narrow factual situations which are not relevant here, and the Quebec statute, the Agricultural Abuses Act, is probably restricted to agricultural lands. Petty trespass legislation in Alberta and Newfoundland requires notice not to trespass by word of mouth or in writing, or by posters or sign boards, before an offence is committed and so poses problems where such notice is given. Legislation in Ontario and Manitoba, however, does not in every case require such notice, and therefore poses the greatest difficulty for surveillance operations. In Ontario, an offence occurred until 1980 when there was unlawful entry upon enclosed land, a garden or lawn, or land on which the entrant has had notice not to trespass; under the new Act there is an offence when there is unauthorized entry onto premises "enclosed in a manner that indicates the occupier's intention to keep persons off the premises". In Manitoba, the offence in part consists of entering into any land or premises which is the property of another and is wholly enclosed.

35. In Chapter 2 of this part, the Criminal Code offence of trespassing at night (section 173) was discussed in relation to surreptitious entries. This offence is equally germane for those who, in the course of conducting surveillance of a house or an apartment at night, "loiter or prowl" near such buildings. If individuals engaged in surveillance merely enter a parking garage to determine the presence of a target's car, and then leave they likely cannot be said to be "loitering" in the sense of "hanging around".[11] Nonetheless, if they

---

[10] The statutes are referred to in Part III, Chapter 2, footnotes 20 to 26.

[11] *R.* v. *McLean* (1970) 1 C.C.C. (2d) 277; 75 W.W.R. 157 (Alta. Mag. Ct.).

enter the garage they may be "prowling", in the sense of "hunting in a stealthy manner for an opportunity to commit a criminal offence" (in this case, mischief, contrary to section 387).[12]

36. Where physical damage, even nominal, occurs to a target's vehicle in the course of an operation, section 387(1)(a) of the Criminal Code, dealing with the wilful damaging of property, may have been violated. In addition, an offence may have been committed under section 388(1) of the Code, dealing with the wilful destruction or damaging of property. It can also be argued that merely handling the vehicle of the target amounts to a trespass upon chattels and is thus an interference with the lawful use or enjoyment of the property contrary to section 387(1)(c). If this is so then the indictable offence of mischief has been committed. Quite apart from possible criminal implications, the tampering with a vehicle, even if it does not result in any damage to the vehicle, may be trespass at common law. The R.C.M.P. position, based on legal advice, is that there is a conflict of judicial authority as to whether trespass to a chattel (a thing) is actionable — i.e. is a wrong — without proof of damage. In our view there is not a conflict of judicial authority,[13] but an absence of judicial authority except for quotations of textwriters by judges. The textwriters quoted assert that in principle trespass to chattels should be no different from trespass to land. In regard to the latter the common law is clear that there may be trespass without damage.

Laws relating to violation of privacy

37. In British Columbia it has been held[14] that a private investigator had not violated the statutory guarantee of privacy by affixing a bumper beeper — a small radio transmitter emitting signals to enable the location of the vehicle to be traced — to the bumper of a car. The car belonged to a husband who was being watched by the investigator pursuant to instructions given by the wife. The court had regard to the fact that the wife was not motivated by malice or curiosity, that she had not attracted public attention, that she had not acted in an offensive manner and that her conduct was therefore reasonable. The use of a "bumper beeper" is probably not in violation of Article 5 of the Quebec Charter of Rights and Liberties of the Person, at least while the vehicle is travelling on public roads. However, it has been argued that attaching such a device to the personal effects or clothes of a person could be a violation. We express no view in that regard.

---

[12] *Ibid.*

[13] The R.C.M.P. position was based on three cases. One was said to support the view that trespass to a chattel is not actionable without proof of damage; but a reading of the case — *Everitt* v. *Martin* [1953] N.Z.L.R. 298 — indicates that the court there went no further than to cast doubt upon actionability without proof of damage. The other two cases cited were Canadian cases: *Demers* v. *Desrosiers* [1929] 2 W.W.R. 241 (S.C. of Alta.) and *Wolverine S.S. Co.* v. *Canadian Dredging* [1930] 4 D.L.R. 241 (S.C. of Ont.). In the first case the court did not decide the point but quoted three English textbooks which suggest that the law is or should be that trespass to chattels is actionable without proof of damage. In the second case the point was not decided.

[14] *Davis* v. *McArthur*, [1971] 2 W.W.R. 142 (B.C.C.A.).

Could surveillance constitute intimidation?

38. To this point we have not discussed the Criminal Code offence of intimidation (section 381). We have no documented instance where such conduct in physical surveillance operations has occurred in the past; therefore, the subject cannot properly be examined as a past practice not provided for or authorized by law. Nonetheless, we raise this offence as a legal issue, if only immediately to discount it, because of its apparent connection with physical surveillance activities in both the Security Service and the C.I.B. The relevant portions of section 381 read:

> 381. (1) Every one who, wrongfully and without lawful authority, for the purpose of compelling another person to abstain from doing anything that he has a lawful right to do, or to do anything that he has a lawful right to abstain from doing,
>
> (c) persistently follows that person about from place to place,
>
> ...
>
> (f) besets or watches the dwelling-house or place where that person resides, works, carries on business or happens to be,
>
> ...
>
> is guilty of an offence punishable on summary conviction.
>
> (2) A person who attends at or near or approaches a dwelling-house or place, for the purpose only of obtaining or communicating information, does not watch or beset within the meaning of this section.

39. Inherent in physical surveillance operations is the following (sometimes persistently) of individuals and observation around buildings, dwelling-houses, etc. It cannot be said, however, except perhaps in a few cases, that the persistent following or watching and besetting has been "for the purpose of compelling another person to abstain from doing anything that he has a lawful right to do, or to do anything that he has a lawful right to abstain from doing". In virtually every case, physical surveillance has involved no "compulsion"; rather it has involved discreet observation of a target. Second, in the few cases where the fact of surveillance has been deliberately made known to the target (for example, in order to frustrate an agent meet) and where therefore there may have been an element of compulsion, the activity in question was almost inevitably not one which the target had a lawful right to perform — the activity might have involved espionage or a criminal operation. Third, it probably cannot be said that surveillance teams, whether C.I.B. or Security Service, have acted "wrongfully" and "without lawful authority" in their pursuit of targets, at least insofar as they have acted in the discharge of their functions as peace officers in combatting crime and countering threats to security.

40. It is thus unlikely that section 381 has been violated by surveillance teams engaged in normal (covert) surveillance activities. The possibility of a violation does exist, however, where surveillance is carried out overtly, for example, in order to deter a domestic group perceived by the Security Service to be a threat to security. In such a case, there is intended to be an element of compulsion

resulting from the surveillance. If the group's activities are lawful, it may be that the Security Service would be acting "wrongfully" and "without lawful authority", thereby violating section 381.

R.C.M.P. attempts to inform provincial governments of legal problems associated with physical surveillance

41. Under this programme carried out early in 1978, the R.C.M.P. held briefing sessions with senior provincial officials in order to inform them of covert investigative techniques which may have contravened provincial statutes. In a letter dated June 6, 1978, Mr. Dare, Director General of the Security Service, reported the results of these briefings to the Solicitor General, the Honourable Jean-Jacques Blais. This letter stated:

> As a result of the Commissioner's instructions of 31 January 1978, the Security Service participated in a number of briefings to provincial Attorneys General on areas where the application of covert investigative techniques may have contravened provincial statutes. Specifically, the objectives, necessity and the consequences of discontinuance of i) alias documentation, ii) dual registration and the use of secret plates for motor vehicles, iii) registration in hotels or other accommodation using an alias.. . .

42. Briefings were carried out as follows:

Newfoundland	— February 3, 1978 — Deputy Minister of Justice briefed by C.I.B.
Nova Scotia	— February 2, 9, 1978 — Director General, Department of the Attorney General, briefed by C.I.B. and Security Service
New Brunswick	— May 11, 1978 — Deputy Minister of Justice and Director of Prosecutions briefed by C.I.B. and Security Service
Quebec	— February 7, 1978 — Deputy Attorney General, Assistant Deputy Minister — Criminal Prosecutions, Assistant Deputy Minister — Police Matters briefed by C.I.B. and Security Service
Ontario	— November 7, 1977 — Attorney General, Solicitor General and Assistant Deputy Attorney General briefed by C.I.B. and Security Service
	— January 11, 1978 — Assistant Deputy Attorney General briefed by C.I.B. and Security Service
Manitoba	— February 6, 1978 — Attorney General briefed by C.I.B. (after C.I.B. consultations with Security Service)
Alberta	— May 8, 1978 — Solicitor General briefed by C.I.B. and Security Service
British Columbia	— January 16, 1978 — Attorney General briefed by C.I.B.

— February 6, 1978 — Deputy Attorney General briefed by C.I.B.

(Note that some of the meetings took place before Commissioner Simmonds' directive of January 31, 1978).

43. There appears to have been no discussion with officials of the Saskatchewan Attorney General's department. Mr. Dare's letter to Mr. Blais explained that the Security Service in Saskatchewan carried out no covert operations which would contravene provincial statutes and that therefore the Attorney General would not be briefed.

44. There appears to have been no mention of possible violations of "rules of the road" under provincial highway traffic legislation or of possible violation of provincial petty trespass legislation during these briefings.

C. NEED AND RECOMMENDATIONS — BRIEF SUMMARY

45. The initial policy issue is whether there is an established need for physical surveillance as an investigative tool for the Security Service and the C.I.B. If so, should changes be made in existing legislation in order to bring effective surveillance operations within the law? Should the changes give surveillance teams special powers so that they may lawfully drive in ways that in the case of other drivers would be offences under provincial or municipal laws? For example, if a member of the Watcher Service exceeds the posted speed limit in order to maintain surveillance of a target should the law be such that he is not guilty of speeding? If the answer is yes, and an accident ensues in which an innocent third party is injured, or his property is damaged, should that person be able to pursue a civil remedy by suing the individual member of the surveillance team, the R.C.M.P., or the federal or provincial governments? If not, should compensation be available through other means?

46. Many, although not all, of the statutes which have been violated during the course of physical surveillance operations might be referred to loosely as being "regulatory" in nature. To some observers, the violation of "regulatory" laws may seem to be unimportant. At least one newspaper commentator has said that breaches of "minor" laws by the R.C.M.P. is not a matter of concern. We disagree. In a national police force, or a security intelligence agency, the adoption of a policy that permits violations of "minor" laws is the thin edge of the wedge. If it is permissible to violate "minor" laws in the public interest (or more accurately, in what the members of the organization *decide* is in the public interest), then an attitude arises that makes it easier to tolerate violations of "major laws". An ethos is created that excuses what is done for noble reasons and asserts its validity. This cannot be acceptable.

47. At the same time, if we, as a democratic society, insist that the police and intelligence agencies, like all government institutions, must be subject to the law, we also wish to ensure that those agencies can perform their assigned tasks effectively. If "minor" laws will be obstacles to that effectiveness, and if a lawful exception to their application can be made *without damage* to the social

purposes of those laws, then the legislators should support amendments to those laws to attain that objective.

48. Physical surveillance operations are indispensable to both services of the R.C.M.P. Present laws pose obstacles for surveillance operations and result in unnecessary violations of the Rule of Law. Existing statutory and common law defences are inadequate. Legislation is needed to provide a statutory defence for individuals engaged in surveillance team operations, in defined circumstances, when their activities contravene some of the laws which restrict such operations at present. Where amendments are necessary in respect of provincial legislation (highway traffic, petty trespass laws etc.), such amendments should be enacted by the provinces concerned. Detailed recommendations are contained in Part V, Chapter 4 and Part X, Chapter 5.

CHAPTER 9

UNDERCOVER OPERATIVES

INTRODUCTION

1. In conducting both criminal and security intelligence investigations, the R.C.M.P. frequently gather information through persons who are not openly identified as members of the Force, or as persons working on its behalf. An undercover operative is often able to approach or infiltrate the subject of interest and so to obtain information which would not otherwise be accessible. The undercover operative may be either a member of the R.C.M.P. or an individual who has volunteered or been recruited by the Force. In the latter case, the individual may already be 'in place' near the target, or may be asked to approach it in his own or in a disguised identity and to gain acceptance.

2. The use of undercover operatives is at once one of the R.C.M.P.'s most effective investigative techniques and the one which causes the greatest difficulty and concern for the Force and the public at large: an undercover operative can gather more important information than any technical or mechanical source, but the nature of his task and the environment in which he must work often create considerable pressure on him to commit unlawful acts.

3. This chapter is devoted to an examination of the use by the R.C.M.P. of undercover operatives and the resulting practices and activities not authorized or provided for by law.

A. ORIGIN, NATURE AND PURPOSE OF THE PRACTICE

4. History abounds with tales of informers. That is true of the Canadian past as much as that of other countries. We described in Part II, Chapter 2, how, in the early days of Confederation, undercover operatives were used by the Dominion Police Force on both sides of the Canada-U.S. border to provide intelligence about the activities and intentions of the Fenians. The primary method of collecting information was to infiltrate informers into Fenian organizations. These undercover operatives often spent years within the organization, in some cases working their way into influential positions. From the early 1870s until the First World War, agents supervised by Commissioners of the Dominion Police continued to play a role in providing intelligence information about politically motivated violence in Canada. Although the North-West Mounted Police did not employ undercover operatives in dealing with the North-West Rebellion of 1885, they did so in policing the Yukon Territory

during the gold rush at the turn of the century. In investigating rumours of American plots to annex the Yukon Territory, the N.W.M.P. used operatives to infiltrate suspect organizations and groups.

5. During the First World War, both the Dominion Police Force and the Royal North-West Mounted Police used undercover operatives in domestic activities related to the war effort. Following the war, both agencies carried out extensive undercover operations to investigate the labour movement. In the years between the World Wars, the R.C.M.P. concentrated its intelligence activities on counter-subversion, frequently using its own members to infiltrate suspect organizations. The major targets of the Force in the late 1930s were Fascist and Nazi political organizations in Canada. One of the most celebrated instances of infiltration by Force members was that of Constable (later Superintendent) John Leopold. In 1921 Leopold managed to infiltrate the Communist Party in Canada. He remained undercover as a member of the Party until 1928, when his true identity was discovered and he was expelled. His testimony was later instrumental in securing the conviction of eight persons as members and officers of the Communist Party of Canada. Upon his subsequent transfer to Headquarters, Leopold began to work full time on the analysis of security files and reports coming in from the field. During the next two decades Leopold would be the R.C.M.P.'s number one resource person on Communism in Canada. He knew many of its leaders in Canada personally, was intimately acquainted with its activities and had a thorough knowledge of its ideology.

6. In criminal matters, individuals operating undercover were first used in earnest after the Second World War. They were deployed primarily in drug investigations, which are a continuing operational priority. The use of long-term undercover operatives for non-drug criminal investigations has never been extensive. The Criminal Investigation Branch has told us that it uses undercover operatives in non-drug investigations ". . . only where circumstances clearly indicate that it is necessary and after all potential results, favourable and otherwise, have been considered".

7. Those who work in an undercover capacity attract a variety of names which obscure the subtle categories into which they fall. Colloquially, undercover operatives are variously called spies, informants or secret agents. The Security Service itself uses the term "human sources" to describe civilian operatives, the more casual of whom are called "contacts".

8. For the sake of clarity we refer to members and non-members undercover as "undercover operatives", even though that expression is not used by the R.C.M.P. There is in fact no umbrella expression used by the R.C.M.P. to cover the various kinds of persons we refer to in this chapter. The general term it uses to describe all non-member operatives is "human sources". The categories into which undercover operatives fall are generally as follows:

(a) the volunteer source;

(b) the undeveloped casual source;

(c) the developed casual source; and

(d) the long-term, deep-cover operative.

While it is not possible to establish iron-clad definitions to cover every possible type of undercover operative, these are the leading distinctions.

The volunteer source

9. The volunteer source does not truly operate undercover. He may be an ordinary citizen who, overtly or otherwise, and often for a single occasion, approaches the R.C.M.P. with information relating to either a criminal or a security intelligence matter. No recruitment or active solicitation is involved, although the criminal investigation officers generally encourage responsible persons to come forward with information about crime, and the Security Service welcomes volunteered information from citizens and others about suspected espionage, subversion or terrorism. Volunteer sources may be motivated by more than good citizenship; they may be seeking favours in exchange for the information they will provide. A criminal may want protection from other criminals, or police intervention with prosecuting authorities in order to recommend a lighter sentence. On the security side, a foreign intelligence officer may furnish information in exchange for assurances of asylum and the provision of a new identity.

The undeveloped casual source

10. By way of contrast, what is called an "undeveloped casual source" may be attracted by solicitation. The approach is invariably low-key and falls short of an intensive "recruitment" but there is nonetheless a degree of active encouragement. Taxi drivers, maintenance or utility personnel, and hotel doormen are typical examples, since their normal tasks provide opportunities to observe targets. Such people are initially interviewed and their co-operation is sought. No reward or payment is offered. If they agree to help, discreet interviews are periodically arranged. Such sources play no covert role and do not disguise their identities by using false documents.

The developed casual source

11. The "developed casual source" differs from the undeveloped source in two respects: the nature of his recruitment and the frequency of contact with his 'handlers'. Before the first approach is made, the R.C.M.P. will assess his interests and decide upon an inducement most likely to attract his co-operation. Most frequently, casual sources recruited by the Security Service provide their assistance out of a sense of loyalty. Inducements may, however, be needed. If the source is a journalist, he could be offered preferred access to stories emanating from the Force. In criminal matters, money may be promised. For those awaiting sentencing, the Force may undertake to speak to the Crown Attorney about the prisoner's "co-operative attitude". The developed casual source will be more likely than his 'undeveloped' counterpart to be assigned an active information gathering role, rather than simply reporting what he sees or hears in the course of his usual activities. Although the source is described as a 'casual', his relationship with the Force may entail regular meetings and last for years. While his affiliation with the R.C.M.P. will be kept secret, his identity is not normally disguised, and he will not normally carry false papers.

The long-term deep-cover operative

12. By far the most intrusive undercover role is that of the long-term, deep-cover operative. Here, both members and human sources commit themselves to extensive, lengthy and often elaborate operations to infiltrate and remain inside a target's sphere. The ultimate long-term, deep-cover operative is the intelligence officer of a hostile foreign power who has been 'turned' by the Security Service into a 'double agent'. Because of the intensity, duration and danger of such operations, long-term, deep-cover operatives are usually paid for their intelligence, although some have worked for ideological reasons alone.

13. In determining whether the person deployed in an operation requiring a long-term, deep-cover operative will be a member or a human source, the R.C.M.P. considers such factors as an individual's ability to penetrate a given target, his trustworthiness, the extent of the control which will be required in handling the operative and the availability of members for the purpose. Since such a person will be committed to the role for periods sometimes as long as several years (and even, rarely, decades), the Force generally prefers to use sources and keep its members available for a greater variety of work.

14. Normally, only undercover members assume false identities for operational purposes. It is extremely rare for a source to use false identification documents during an operation, although such documents may be needed in order to protect him at a later stage from vindictive targets. For the most part, sources are chosen because of an existing personal history which allows them to approach a target without arousing suspicion. For example, the source might 'espouse' a philosophy similar to that of the target. The source used by the Security Service to penetrate the Western Guard (discussed below) was chosen on this basis.

15. Where members assume false identities for long-term, deep-cover work, they are provided with a fabricated life history, including such invented details as the names of schools and churches attended, former employment and previous addresses. These 'legends' are given credibility through identity cards, driver's licences and S.I.N. numbers which reflect the legend. No effort is spared to give every appearance of genuineness to the elaborately fabricated story, since some targets thoroughly investigate the personal histories given by prospective adherents; the consequences of detection could be grave. With his legend in place, the undercover member develops a cover story which gives the appearance of legitimacy to his approach to the target.

16. It is not uncommon that the long-term, deep-cover operative is compelled to dissociate himself for considerable periods from family and friends in order to perform his role. Such isolation, taken with the stress and danger often associated with undercover work, creates a need for able, dependable and firm handling by experienced members. A bond develops between the operative and his handler in such circumstances: a dependence arises which is virtually parental. The dynamics of the relationship must be anticipated and understood if control of the operative is to be maintained. Where control is lost, the operative is withdrawn.

17. Long-term, deep-cover operatives may require extensive training in the 'tradecraft' of spying. Theirs are the most sophisticated of operations, necessarily so because of the sophisticated nature of their targets, whether hostile intelligence agencies or organized criminal groups.

The use of undercover operatives

18. The general manner of using undercover operatives in the Security Service differs significantly from their use in criminal investigations. In the latter they are used mainly to obtain evidence for prosecutions, of which drug related charges form a significant part. Consequently, sources in criminal investigation work, like undercover members in such work, expect that their relationship with the R.C.M.P. will be exposed (or, in the vernacular of security and police work, that they will be 'burned') in a relatively short time — a matter of perhaps months, not likely more than a year. However, the Security Service seldom uses sources primarily for the collection of evidence for use in court; in the vast majority of cases the hope of the Security Service is that the source will provide information over a matter of at least months and frequently years without being 'burned'. One such case came to public attention with the testimony of Warren Hart before this Commission. Mr. Hart testified that he had been recruited by the R.C.M.P. from the United States and directed to infiltrate a radical Black movement in Canada. A false immigration record was arranged for him in order to enhance his credibility. Mr. Hart succeeded in penetrating the movement and related information to the R.C.M.P. while posing as a bodyguard for Roosevelt Douglas, one of the leaders of the movement.

19. If the source acquires information which is evidence of a crime, the Security Service may decide to lay charges, in which case it will do its utmost to preserve the 'cover' of the source by encouraging the police to obtain the same or other evidence by their own means. If that approach succeeds, the source will not have to testify and can thus continue to operate as a source in the same group or at least in the same milieu. The security intelligence agency's source will in any event not always acquire evidence of a crime. Even if he does acquire such evidence, for example, evidence of espionage, the main interest of the Security Service will not ordinarily be to prosecute the foreign intelligence officer who may have committed the offence. An attempt may be made to 'turn' the intelligence officer into a double agent or to have him declared *persona non grata* by the Department of External Affairs, or otherwise to neutralize his effectiveness while at the same time preserving the source's cover.

20. The practice of using undercover operatives in police and security intelligence work is well established in Canada and represents an important and valuable technique in criminal and security investigations. In the Supreme Court of Canada decision in *Kirzner* v. *The Queen*, Chief Justice Laskin referred to the use of spies and informers as "an inevitable requirement for the detection of consensual crimes and of discouraging their commission."[1] The Home Office in England expressed similar sentiments in a 1969 statement:

[1] [1978] 2 S.C.R. 487 at p. 493.

If society is to be protected from criminals, the police must be able to make use of informants in appropriate circumstances. Informants, appropriately employed, are essential to criminal investigations...[2]

21. The Report of the Canadian Committee on Corrections stated that:

> One of the most important aspects of police work in the field of crime prevention and the detection and apprehension of offenders involves the gathering of information with respect to intended crimes and the organization of criminal groups.
>
> ...Traditionally, information as to intended crimes has been obtained from informers and undercover agents.[3]

22. In a recent statement, Mr. Philip B. Heyman, Assistant Attorney General, Criminal Division of the United States Department of Justice, referred to undercover techniques as a "... minimally intrusive, powerfully effective weapon to detect, combat and deter the most serious forms of crime...".[4]

23. United States Attorney General Edward Levi, in 1976, noted in setting forth guidelines on F.B.I. use of informants in domestic security and criminal investigations that informants may often be essential to the effectiveness of properly authorized law enforcement investigations.[5] A number of other American studies have stressed the importance of the human source in criminal, particularly drug, investigations.[6]

24. In the R.C.M.P. Security Service, the use of undercover operatives is greatest in investigating domestic groups in Canada. A senior Security Service official stated to us, in the course of a briefing on the subject in February 1980, that undercover operatives are the "bread and butter" of Security Service operations. The vital importance of information provided to a security intelligence agency cannot be stated better than it was by the Royal Commission on Security:

> 285. All security activities depend upon information. The adequacy of appreciations and judgments can be no better than the information available. Without accurate and full information, the perception of the threat by the security authorities, and thus by the government whom they advise, will be less than satisfactory. Unimportant threats may be overemphasized, significant threats may be overlooked, and vital counter-measures may not be taken.

---

[2] The guidelines were contained in the *Home Office Consolidated Circular to the Police on Crime and Kindred Matters*, (Section 1, para. 92).

[3] Report of the Canadian Committee on Corrections, *Toward Unity: Criminal Justice and Corrections*, Ottawa, 1969, at p. 75.

[4] Testimony before the Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary — House of Representatives (March 4, 1980).

[5] *Attorney General's Guidelines for F.B.I. Use of Informants in Domestic Security, Organized Crime, and Other Criminal Investigations*, Washington, December 15, 1976.

[6] See e.g., J.H. Skolnick, *Justice Without Trial: Law Enforcement in Democratic Society*, New York, John Wiley & Sons, 1966, at p. 133; J. Wilson, *The Investigators: Managing F.B.I. and Narcotics Agents*, New York, Basic Books, 1978, at p. 58.

> 288. Human agents are one of the traditional sources of intelligence and security information, and any security service is to a large extent dependent upon its network of agents, on the scale of their penetration of or access to useful targets and on their reliability. Operations involving human sources require the most sophisticated handling by trained men with wide experience. Nevertheless, in spite of the difficulties associated with some of these operations, we regard them as essential to an effective security posture. We would go further, and suggest that it is impossible fully to comprehend or contain the current threats to security — especially in the field of espionage — without active operations devoted to the acquisition of human sources.[7]

We accept and endorse these statements emphasizing the utility of undercover operatives. Next we turn to violations of the law that have stemmed from these undercover operations during recent years. Before proceeding, however, we wish to note that since the Supreme Court of Canada's judgment in the *Kirzner* case there has been a view at very high levels of the R.C.M.P. that Chief Justice Laskin's language in that case is authority for the commission of offences by R.C.M.P. informers. In our opinion there is nothing in Chief Justice Laskin's judgment that supports the view that illegal conduct by an informer is or will be countenanced by the law.

B. LEGAL AND POLICY ISSUES ARISING FROM THE ACTIVITIES OF UNDERCOVER OPERATIVES

25. In this section, we shall examine possible violations of federal, provincial and municipal laws which may have been committed in the course of undercover operations and civil wrongs which may have occurred during such operations. These potential illegalities fall within the following general categories:

(a) violations of laws which require the accurate identification of persons and property;

(b) breaches of statutes such as the Income Tax Act, the Canada Pension Plan Act, and the Criminal Code arising out of payments made to sources and the encouragement of sources not to declare as income payments received from the Force for work on its behalf.

(c) violations of the Criminal Code and provincial laws during acts done to gain acceptance or maintain credibility with target groups;

(d) the breach of statutory prohibitions against possession and delivery of controlled or restricted substances or narcotics by undercover operatives investigating drug offences;

(e) violations of laws forbidding breach of trust by public officers and interference with confidential relationships as a result of practices connected with the recruitment and treatment of sources;

(f) offences under the Criminal Code which may occur through the removal of the property of others by an undercover operative and its delivery to the police;

(g) civil wrongs.

---

[7] *Report of the Royal Commission on Security*, Ottawa, 1969.

Each of these areas will be considered separately.

(a) *False documentation and registration*

26. In the previous chapter we examined the use of false identification documents (support documentation) in relation to physical surveillance operations, where such documents were needed to maintain an operation's secrecy. An even greater need for support documentation arises in the use of undercover operatives. Some targets of the Security Service and, increasingly, suspects in criminal investigations go to considerable lengths to verify the identity of individuals who seek to gain access to their organizations. Convincing support documentation is essential. To disguise effectively an operative's identity is not only a strategic necessity, it is essential for the physical safety of the operative, both during the actual operation and afterwards when it is sometimes necessary to relocate a threatened operative and to provide him with a completely new identity. We may comment further in a future Report on the need to protect the identity of sources, but at this time we withhold our comments pending the decision of the Supreme Court of Canada in *Solicitor General et al* v. *The Royal Commission of Inquiry with respect to the Confidentiality of Health Records in Ontario et al.*[8]

27. As explained earlier, the need for false documentation arises primarily in long-term, deep-cover operations. Casual sources do not ordinarily disguise their true identities; only their affiliation with the R.C.M.P. is kept secret. There is nonetheless an occasional need for false identification even for casual sources. When meeting, frequently in hotels, sources and their handlers have misrepresented their identities in order to avoid detection by their targets, who may have checked hotel registers and bribed hotel managers in order to obtain information about encounters with Criminal Investigation Branch or Security Service officers. Meetings between a member of the Security Service and a potential defector provide one example of the type of operations which have been kept secret, both for diplomatic and operational reasons.

28. The kind of support documentation used varies with the operation involved. Several common types of false documentation have been brought to our attention. They include:

— driver's licences
— S.I.N. cards
— passports
— credit cards
— motor vehicle registrations
— licence plates
— birth certificates
— education certificates

[8] The decision of the Ontario Court of Appeal, dated May 10, 1979, has not been reported.

29. The use of false documentation has resulted in the commission of a number of offences by undercover operatives, and by their handlers. These offences relate primarily to provincial highway traffic legislation (drivers' licences, licence plates, vehicle registrations), provincial hotel registration legislation (requiring registration in the guest's proper name) and a number of Criminal Code offences relating to forgery. In the previous chapter we examined in some detail these same legal difficulties as they arose in the context of physical surveillance operations. The issues here, for the most part, are identical, except that the broader range of identification documents necessary for undercover operatives means that more statutes may have been violated. In addition, one offence that we did not consider a problem in physical surveillance operations poses one in undercover operations because of the greater variety of cover or support documentation needed. It arises when documents for undercover operatives may have been obtained to substantiate the operative's cover story as to his date and place of birth, his supposed marriage etc.. If the documents were forged or if the documents were obtained through making a false statement in an application, and a record of such false information was inserted in a register, an offence may have been committed by those who caused the entry to be made. Section 335 of the Criminal Code reads:

> 335. (1) Every one who unlawfully
>
> (b) inserts or causes to be inserted in a register. . . an entry, that he knows is false, of any matter relating to a birth, baptism, marriage, death or burial, or erases any material part from such register...
>
> ...
>
> is guilty of an indictable offence and is liable to imprisonment for five years.

(b) *Complying with fiscal statutes relating to employer-employee relationships*

(i) Non-declaration of income and non-payment of tax

30. Sources may have been given a number of concessions in exchange for their assistance. The payment of money is a practice by police and security forces in many countries. The Security Service policy reflects the widespread acceptance of this practice:

> The secret expenditure of public funds on human source operations is recognized as a legitimate and necessary practice in the pursuit of intelligence gathering. It would not be possible to acquire a sufficient number of sources without provision to compensate them for their efforts and expenses.

Yet payments to sources threaten to reveal their covert role. Hence, care has been taken to ensure that payments do not attract attention. While the C.I.B. has no policy in this regard, Security Service policy until 1977 had been that sources should be instructed never to include payments in calculating taxable income. The policy read:

> All sources should be warned that any monies received from the Security Service must *never* be declared as income on their income tax returns. However, if part or all of such monies is retained in a manner which pays interest, such interest must be declared to avoid the attention of the tax department.

The policy was cancelled in November 1977, when its propriety came under review.

31. It is an offence under section 239(1) of the Income Tax Act for an individual to make false or deceptive statements in his income tax return. Where Security Service officers have advised their sources not to declare payments from the Force as income, those officers may have committed an offence.

(ii) *Employment relationship betwen R.C.M.P. and sources*

32. There are other statutes which require an employer to deduct money from remuneration due and to remit it to government. An example is the Canada Pension Plan Act. The R.C.M.P. has acted as if no source is ever an employee for the purposes of such statutes. While we have no doubt that that view is correct in law in regard to most sources, we also are convinced that in some cases a source is an employee of the R.C.M.P. within the meaning of the general law and the statutes in question. For example, Warren Hart was a paid full-time source of the R.C.M.P. Security Service from 1971 to 1975. We think that the tests that the law applies to determine whether a person is an employee (not an independent contractor) were satisfied in his case: the Security Service could order or require what was to be done, as to the details of the work; his work was an integral part of the "business" of the Security Service, not merely accessory to it; he was "part and parcel of the organization"; and he put his personal services at the disposal of the R.C.M.P. during some period of time and did not merely agree to accomplish a specified job or task.[9] We consider that the R.C.M.P. should address these issues in this light and recognize that non-payment and non-disclosure, particularly in the case of full-time sources, may give rise to breaches of the law. In Part V, Chapter 4 we shall make recommendations that the government should seek legislative amendments to overcome these practical difficulties — amendments similar to those referred to above in regard to the declaration of income tax.

(c) *Acts done to gain acceptance or to maintain credibility*

33. The most significant and intractable problem which arises in undercover operations, particularly those carried out by the Security Service, is the commission of unlawful acts by operatives in order to gain or maintain acceptance by the targetted individual or group. Sometimes, it is only by

---

[9] These tests are found in such cases as *Collins* v. *Herts County Council* [1947] K.B. 598; *Lambert* v. *Blanchette* (1926) 40 Q.B. 370 (Que. C.A.); *Stevenson London and Harrison Ltd.* v. *Macdonald and Evans* [1952] 1 T.L.R. 101 at 111 (Eng. C.A.); *Bank Voor Handel en Scheepwaart* v. *Stratford* [1953] 1 Q.B. 248 at 295 (Eng. C.A.); *Alexander* v. *M.N.R.* [1970] Ex. C.R. 138 at 153 (Exch. Ct.).

engaging in such conduct that the operative will advance to responsible positions within a target group, and therefore increase his access to valuable information.

34. A useful example is afforded by a case which came to public notice in 1977 when a long-term, deep-cover operative placed by the Security Service gave evidence at the trial of criminal charges laid against leaders of the Western Guard Party. The Western Guard Party professed an extreme ideology of which the chief tenets were racism, anti-Semitism and strident anti-Communism. It was suspected of being responsible for a rash of spray paintings which had defaced public and private property in Toronto in the early and mid-1970s. More seriously, the Security Service suspected in 1975 that the Western Guard planned to disrupt the 1976 Olympic Games, some of which were to be held in Toronto. That the Toronto segments included a soccer game involving the team from the State of Israel lent a particular urgency to the investigation. The Security Service recruited Robert Toope, who had come to its notice by reason of stories in the press concerning his anti-union activity at his place of business. With a view to using that publicity as a foundation for his cover story in applying to join the Western Guard, the Security Service sent Mr. Toope to Western Guard headquarters, where he was accepted and given membership. Mr. Toope testified at the trial of the accused that his involvement in the Western Guard Party fell roughly into four phases:

(i) The first phase included his initial penetration, his acceptance as a member and then as a group leader, his involvement in the distribution of the Guard's literature and then in pasting its posters on public sites, all of which occurred between May and September or October 1975.

(ii) Immediately thereafter, two events occurred which signalled the second phase of his penetration, deepened his involvement and led to his participation in acts and conspiracies of a more serious sort. The first event was the arrival of one "A", a new member who had a penchant for aggressive, violent behaviour. The second was the issuance of instructions by the Guard's leader to engage in a broader category of crime. Thereafter and through the late autumn of 1975 until February of 1976, Mr. Toope took part with "A" in spray painting incidents, and acted as a driver on occasions when "A" threw bricks through windows. As Mr. Toope became more and more concerned about "A's" propensity for violence and his increasingly uncontrollable behaviour, he expressed to his handler a desire to reduce his involvement. As a result, in about February of 1976, Mr. Toope told the Guard's leader that he no longer wished to accompany "A" on his missions. He gave as his excuse his concern for his family's welfare should he be caught.

(iii) In the weeks following, the quantity and quality of Mr. Toope's information waned. In about March 1976, the source and his handler decided that he should broaden his role again, but within certain limits. Specifically, it was agreed that Mr. Toope would attempt not to go out with "A", but rather would try to involve other members in such expeditions, with the hope that the presence of others would discourage "A's" impulsive and

dangerous tendencies. As well, Mr. Toope and his handler agreed that if he was to be involved at all in acts such as throwing objects through windows, his involvement would be strictly limited to driving the others to the scene.

(iv) In this fourth and last phase of Mr. Toope's involvement, he won once again the trust and confidence of the group. He was therefore able to obtain information which led to the arrest of the members before they had an opportunity to disrupt the Olympic soccer game at Varsity stadium. The Guard group had planned to throw smoke bombs onto the field during a game between the Israeli team and a team from South America.[10]

35. While unlawful acts to gain admission or enhance credibility pose problems in undercover operations on both the criminal investigation and Security Service sides of the Force, senior officers in the criminal investigation side have reported that such violations in their work have been limited primarily to drug investigations, and result from the narrowness of the statutory exemptions available in the Narcotic Control Act and the Food and Drugs Act for police and persons acting pursuant to their instructions. (For a discussion of those violations, see below.)

36. In order to determine the extent and prevalence of such unlawful acts on the Security Service side, the Commission asked the present Deputy Director General (Operations) of the Security Service to request certain Area Commanders in the Security Service to assess the frequency with which such violations have occurred in the past, and to give their opinion whether undercover operatives need to violate laws in order to work effectively. At our request a message to this effect was sent on February 22, 1980 to certain Area Commanders. We selected those Area Commands because they have been the areas in which most use has been made of undercover operatives in the past two decades, and they would therefore be the Area Commands most likely to be able to give us evidence as to "extent and prevalence". It asked how often in the past 20 years there had been a "real need" for undercover operatives to commit criminal acts, and whether there had been intelligence operations which could not be commenced because criminal acts were known to be required of new members in the target group. Area Commanders were also asked to survey members in their command and ex-members in order to identify cases which would illustrate the extent and prevalence of violations.

37. One Command identified eight operations in which undercover operatives had either committed violations or had been asked by the target group to do so. The violations included mischief to property, fraud, failure to declare income, and theft under $200.00. In one case, the source had been asked to obtain certain articles the possession of which is illegal. The source was instructed by his handlers to obtain some of the items and abided by that instruction. The source was not instructed regarding others because his handlers were confident that he would not become involved in the matter. In another case a source was

[10] Trial transcript, *Regina* v. *Andrews et al*, Criminal Assizes Court, Judicial District of York (Toronto, Ontario), 1977, before His Honour Judge Graburn and a jury.

asked by a target group to participate in a financial fraud. Group leaders eventually decided to involve a different individual, and it appears that in any event the fraud did not take place.

38. Another Area Command identified two cases in response to the inquiry from Headquarters. In one, an undercover operative committed theft under $200.00 in order to enhance his acceptance by a target group and was later credited with preventing the commission of a serious crime. In the second case, an undercover operative was directed by the target group to plan and carry out a physical assault upon an enemy of the group. When the advice of Headquarters was sought by the field office involved, indirect steps were counselled which would discourage the group leaders from pressing the attack, but it was acknowledged by one senior officer that it might well be necessary for the operative to carry out a simple assault in order to maintain his cover. The Area Command has advised us that "there is no indication on the source file that this was ever pursued further".

39. Another Area Command reported no new cases, saying that all such operations were already before this or other Commissions.

40. We have encountered additional cases in which undercover operatives have violated laws. In some, operatives took part in illegal demonstrations. In others, they purchased or possessed restricted weapons; purchased and possessed explosives without appropriate permits; obtained access to confidential information in contravention of the governing statute; committed mischief in relation to private and public property and caused wilful damage to property.

41. We wish to remark in particular about a practice which is common to both the Criminal Investigation Branch and the Security Service — participation by the undercover operative in the planning of a crime. From our reading of its policies, we have observed that the R.C.M.P. has been concerned that such conduct itself amounted to a violation of law (as the offence of conspiracy). We consider that such conduct is not unlawful so long as the operative does not intend to take part in the act being planned. The Supreme Court of Canada in *Regina* v. *O'Brien*[11] held that a mere agreement to commit an indictable offence, without the intention to carry into effect the common design, is not sufficient to constitute the offence of conspiracy. For the operative to commit the offence of conspiracy, therefore, he would not only have to agree but also to intend to put the common design into effect. If the rest of the conspirators did so intend, they could be convicted of conspiracy.

(d) *The Food and Drugs Act*[12] *and the Narcotic Control Act*[13]

42. In drug investigations, an undercover member or source necessarily adopts the guise and mannerisms of individuals who typify the drug community. In the course of playing the part of an addict or trafficker, the undercover operative may be asked to handle, administer or deliver drugs. Criminal

[11] [1954] S.C.R. 666.
[12] R.S.C. 1970, ch.F-27.
[13] R.S.C. 1970, ch.N-1.

investigation officers have repeatedly stressed that such acts are essential to attaining and maintaining credibility in the drug community. However, under existing law, such acts may, depending on the circumstances, result in the commission of drug offences by the operative.

43. Drug offences are defined in the Narcotic Control Act and the Food and Drugs Act. Section 3 of the Narcotic Control Act prohibits the possession of a narcotic. Section 4(1) of the Act provides that "no person shall traffic in a narcotic or any substance represented or held out by him to be a narcotic". Section 4(2) provides that "no person shall have in his possession any narcotic for the purpose of trafficking". The expression "traffic" means "to manufacture, sell, give, administer, transport, send, deliver or distribute", or to offer to do any of these activities. Section 5 of the Act states that except as authorized by this Act or the regulations, "no person shall import into Canada or export from Canada any narcotic". Section 34(1) of the Food and Drugs Act prohibits trafficking in a controlled drug or any substance represented or held out to be a controlled drug. Possession of any controlled drug for the purpose of trafficking is prohibited under section 34(2). In this section, the expression "traffic" means "to manufacture, sell, export from or import into Canada, transport, or deliver", otherwise than under the authority of Part III of the Act or the regulations. There is no offence of possession of a controlled drug *simpliciter*. Under section 41(1), it is an offence to possess a restricted drug. Section 42(1) prohibits trafficking in a restricted drug or any substance represented or held out to be a restricted drug, and section 42(2) prohibits possession of a restricted drug for the purpose of trafficking. The expression "traffic" has the same meaning as it does in the context of controlled drugs.

44. We now examine a number of problem situations which arise in connection with drug investigations as such problems were presented to us in meetings with senior officers from the R.C.M.P.'s Criminal Investigation Branch.

(i) The Commission or Kickback/Trafficking Situation: In making a purchase of narcotics directly from, or as a result of an introduction by a middleman, the undercover operative frequently has been expected to comply with the custom of the trade by giving a small percentage of the purchase to the middleman as a commission. Under present legislation, the undercover operative would be committing the offence of trafficking.

(ii) The Administering/Trafficking Situation: In the course of their associations with addicts, undercover members or sources (the latter of whom may themselves be addicts) have been asked by the addict to administer or assist in administering the drug. As in the "kickback" situation described above, administering a drug may constitute the offence of trafficking.

(iii) The Passing On/Trafficking Situation: Again, because of their required association with drug users, undercover operatives have been called upon to "take a joint" of marijuana, sniff cocaine, or even inject heroin. Undercover members have been instructed to simulate the act where possible or, if necessary, refuse the drug and pass it on. By passing on the drug, the undercover member may commit the offence of trafficking. Undercover sources, who may be regular users in any event, have been

given no instructions to simulate the use of the drug. Nonetheless, in passing on the drug, they may also have committed the offence of trafficking.

(iv) The Offering/Trafficking Situation: As part of establishing and maintaining credibility, undercover members have been *encouraged* to offer drugs for sale, but never to carry through such an offer by actually making a sale. This has been a regular operational practice. Undercover sources (who are sometimes established traffickers) have generally been allowed to operate as they normally would. Often this has meant that sources are permitted to continue their possession or trafficking of drugs. In the case of both members and sources, the offence of trafficking may have been committed.

(v) The Distribution/Trafficking Situation: The "controlled delivery" of narcotics is another operational technique which has raised questions of legality. In order to gain sufficient evidence or intelligence to implicate the principals in illicit drug organizations, decisions have been made to "sacrifice" an amount of drugs (normally only a small amount) for distribution to users in order to avoid the target's suspicion that would arise when a quantity of drugs destined for the "market" did not arrive. Evidence led at a recent British Columbia Supreme Court drug trial illustrates this operational technique.[14] C.I.B. handlers, after taking samples of a drug supplied to their source by the target, permitted the source to sell the remainder of the drug for this very reason. 'Sacrifices' have also occurred in 'Test Run' situations, where an international drug enterprise, having set up a major deal with an undercover operative to import drugs into Canada, will first run a comparatively small amount through the planned route before delivery of the main shipment. Where undercover operatives have become directly involved as couriers, they may have committed the offences of importing and trafficking.

(vi) Possession: Section 3(1) of the Narcotic Control Regulations[15] states in part:

> 3. (1) A person is authorized to have a narcotic in his possession where that person has obtained the narcotic pursuant to these Regulations and...
>
> (g) is employed as an inspector, a member of the Royal Canadian Mounted Police, a police constable, peace officer or member of the technical or scientific staff of any department of the Government of Canada or of a province or university and such possession is for the purposes of and in connection with such employment.

The apparent breadth of section 3(1) is limited by the requirement that the narcotic be obtained "pursuant to these Regulations". We do not think that when an undercover member comes into possession of a narcotic while investigating narcotic trafficking, he is protected by this section. While the member does have possession "for the purposes of and in connection with such

[14] Reported on appeal in *Regina* v. *Ridge*, (1979) 51 C.C.C. (2d) 261 (B.C.C.A.).
[15] C.R.C., ch.1041.

employment", he has not obtained the narcotic "pursuant to these Regulations". The Regulations provide protection only in the specific case of an R.C.M.P. member being supplied the narcotic by a licensed dealer (section 24(2)). A provision similar to section 3(1)(g) is included in the part of the Food and Drugs Regulations[16] dealing with restricted drugs. (It will be recalled that there need be no corresponding exemption in the case of a *controlled* drug, as possession of that drug is not an offence):

> J.01.002. The following persons may have a restricted drug in their possession:
>
> (c) an analyst, inspector, member of the Royal Canadian Mounted Police, constable, peace officer, member of the staff of the Department of National Health and Welfare or officer of a court, if such person has possession for the purpose and in connection with his employment.

Unlike the Narcotic Control Regulations, however, the Food and Drugs Regulation does not cover possession by sources. In addition to the exemptions described above for the possession of a narcotic, the Minister may, pursuant to the regulations, authorize possession of a narcotic as follows:

> 68. (1) Where he deems it to be in the public interest, or in the interests of science, the Minister may in writing authorize
>
> (a) any person to possess a narcotic,
>
> for the purposes and subject to the conditions in writing set out or referred to in the authorization.

These authorizations for possession of narcotics and restricted drugs must, however, be read in light of the comments of Mr. Justice Laskin, when he was still a member of the Ontario Court of Appeal, in *Regina* v. *Ormerod*.[17] At that time, the Regulation read as follows:

> An inspector, a member of the Royal Canadian Mounted Police, constable or peace officer or member of the technical or scientific staff of any department of the Government of Canada, of a Province or university, may be in possession of a narcotic for the purpose of, and in connection with, his employment therewith.

His Lordship limited the effect of the section (now section 3(1)(g) of the Narcotics Control Regulations, and similar to section J.01.002 of the Food and Drugs Regulations) by holding that the Regulation did not protect an undercover member of the R.C.M.P. who had purchased narcotics and therefore had "possession as a direct consequence of trafficking which ensues from solicitation by a policeman".[18] It may be argued nonetheless that the member and even his source would have a defence if charged with possession since the courts have held the offence of possession to involve a degree of *control* which would not be present if the possession was solely for the purpose of furthering the investigation and the person in possession had the immediate intention of turning the drug over to the police. In long-term undercover operations,

---

[16] C.R.C., ch.870.

[17] [1969] 4 C.C.C. 3, at p. 13.

[18] *Ibid.*, at p. 240.

however, it is not always the member's or source's immediate intention to turn the drug over to the police. The six operations described earlier in this paragraph, although they may be unlawful, have been referred to us by the R.C.M.P. as vital to the successful prosecution of drug-related offences.

(e) *Breach of trust and interference with confidential relationships*

(i) Section 111, Criminal Code of Canada

45. When a source who is the employee of a government discloses information which he is bound by his office to keep in confidence, the issue arises as to whether the source has thereby committed a breach of trust as that offence is defined by section 111 of the Criminal Code.

46. The concept of "breach of trust" in this context is very elastic and flexible. It includes any malfeasance in office. The leading case on the subject in Canada is *Regina* v. *Campbell*,[19] a decision of the Ontario Court of Appeal. That Court emphasized that there may be guilt even for negligence. From this it follows that it is not essential, in order to obtain a conviction, that the official have the intent to injure the government. In our view all that the prosecution need prove is that the official intended to do the act complained of — i.e. the communication of the information. It follows that it would be no defence that the official believed that he was acting in the public interest, or in the interest of national security. In *Regina* v. *Arnoldi*,[20] Chancellor Boyd said:

> The gravity of the matter is not so much in its merely profitable aspect as in the misuse of power entrusted to the defendant for the public benefit, for the furtherance of personal ends. Public example requires the infliction of punishment when public confidence has thus been abused. ...

Thus, payment for the information would enhance the probability that a prosecution would result in conviction. A source in government, paid monthly by a security intelligence agency for the provision of confidential information received by him because of his public position, would likely be guilty under this section unless the information were evidence of the commission of a crime. (In the latter case he would be carrying out a citizen's duty that is recognized by the law.) However, payment would not be necessary for conviction. It simply makes conviction more likely because the payment of money would lessen the possibility that a jury would be impressed by the protestation of the defence that what the official did was for love of country.

47. The foregoing conclusion applies whether the government in question is federal, provincial or municipal, provided that the information is of a type which it is his duty not to divulge. If the government in question were a provincial government, and the security intelligence organization asked an official of that government to report to it information concerning that government's dealings with foreign powers, no doubt it might be contended on behalf of the security intelligence organization, and on behalf of the official if he were prosecuted, that he was providing information concerning matters which, in the

[19] [1967] 3 C.C.C. 250.

[20] (1893), 23 O.R. 201 at p. 212.

circumstances, were not legitimate operations of a provincial government and were within the sole legitimate concern of the federal government. However, while a jury might not convict if it were satisfied that the official's concern was genuinely limited to protecting Canada against unacceptable foreign intervention, we still think it probable that an offence is committed in those circumstances.

48. Moreover, the information provided may inevitably stray from the narrow limits intended and include other confidential information about perfectly proper provincial government plans and policies. Plans and policies might be disclosed which concern matters under negotiation or future negotiation with the federal government, or the negotiations of provincial governments with foreign governments or private interests concerning economic matters. In that event, the argument that there is no offence committed evaporates, and in addition there is a very serious constitutional and political issue of a policy nature involved if the federal government through its security intelligence agency obtains confidential information about the policies and plans of a provincial government.

49. If an offence is committed by such a source, the members of the security intelligence organization handling the source, encouraging the source to provide such information and perhaps even paying him a regular honorarium, would be guilty either of conspiracy or of being accessories to the offence itself.

50. A second problem presented by section 111 arises when the R.C.M.P. refrains from bringing criminal charges so as not to compromise undercover operations.

51. Undercover operations often allow the R.C.M.P. to learn about crimes which the target has committed or plans to commit, but it is not always consistent with the objectives of the investigation immediately to arrest and charge the target with the known or anticipated offence or conspiracy. For example, an undercover operative in a drug investigation may observe scores of violations of drug laws among those he has infiltrated, but his handler may decide to await a larger, more serious transaction before arranging the arrest of those responsible. Even then, some offenders may never be charged, because the Force intends to use them as unwitting tools in order to acquire evidence against "more important" offenders. This practice is known as "targetting upwards". On the security side, an operative may report on crimes committed by a target over a period of years without charges being laid, since the object of his mission may be to obtain continuous intelligence information about a long-term threat to security.

52. All R.C.M.P. members are sworn to an oath of office which requires them both to obey their lawful orders and "faithfully, diligently and impartially" to perform their duties. Since their duties include those assigned to peace officers in the preservation of peace, the prevention of crime and offences against the law and the apprehension of criminals and offenders, the question arises whether they violate section 111 by enforcing laws "selectively". Section 111 of the Criminal Code of Canada reads as follows:

> Every official who, in connection with the duties of his office, commits fraud or a breach of trust is guilty of an indictable offence and is liable to imprisonment for five years, whether or not the fraud or breach of trust would be an offence if it were committed in relation to a private person.

The Supreme Court of Canada has held that section 111 of the Code applies to a person who holds an office within the definition of that word in section 107[21] and also a person holding an office within the usual meaning of the word "office". The Court took notice of the broader dictionary definition which is, in part, "A position of duty, trust or authority, especially in the public service, or in some corporation, society or the like" (per Chief Justice Fauteux, in *Regina* v. *Sheets*[22]). It is therefore beyond doubt that a member of the R.C.M.P. is an "official" within the meaning of that word as used in section 111 of the Code. Given that fact, is omitting to enforce the criminal law immediately upon learning of each and every crime a "breach of trust... in connection with the duties of his office..."?

53. The phrase "breach of trust" as it appears in the section has been given a broad, non-technical interpretation by the Courts. Its meaning is not confined to the rules and concepts of the law of trusts and fiduciaries. Nor is there any requirement that there be a "trust property". In the case of *Regina* v. *Campbell*,[23] the Court of Appeal for Ontario said:

> In our opinion s.103 [now 111] is wide enough to cover any breach of the appropriate standard of responsibility and conduct demanded of the accused by the nature of his office as a senior civil servant of the Crown... The question which will have to be determined and which has not been considered is whether Campbell by reason of his dealings and actions abused the public trust and confidence which had been placed in him by his appointment as a servant of the Crown and thereby did he or did he not commit a breach of trust in relation to his office?

A later passage in the same judgment makes it clear that the Court of Appeal accepted the term "trust" in its widest sense:[24]

> The situation has been very tersely summed up in the United States. For example, in the American Words and Phrases, Permanent Edition, Vol. 29, p. 250, there is the following note:
>
> "An 'office' has been defined as 'a special trust or charge created by competent authority'; more tersely still 'a public office is a public trust.' ... *Gracey* v. *City of St. Louis*, 111 S.W. 1159, 1163."

---

[21] Section 107 defines "office" as follows:

> "office" includes
>
> (a) an office or appointment under the government,
>
> (b) a civil or military commission, and
>
> (c) a position or employment in a public department,

[22] (1971) 1 C.C.C. (2d) 508 at 513.

[23] [1967] 3 C.C.C. 250.

[24] *Ibid.*, at p. 257.

> The respondent suggests that the possible use of the word "trust" to implicate "confidence" is a colloquial usage. While it is perfectly true that the term "trust" is a term of art in the legal field of equity the Shorter Oxford Dictionary at p. 1362, gives the following meaning for the word "office":
>
> 4. A position to which certain duties are attached, especially a place of trust, authority or service under constituted authority, M.E. e.g. The Office of Coroner.

54. There are many ways in which a public official can breach his trust in office. He may accept a bribe, or neglect his job through laziness. Those types of breach of trust are not relevant to the present discussion. Rather, the question for present consideration is whether a deliberate omission to enforce the law in certain circumstances may constitute a breach, notwithstanding that it is motivated by the honest belief by the officer that he is acting in the best interests of the public.

55. The English Court of Appeal has had occasion in recent times to consider this question in *R.* v. *Metropolitan Police Commissioner, ex parte Blackburn*, (Blackburn No. 1)[25] and *R.* v. *Metropolitan Police Commissioner, ex parte Blackburn*, (Blackburn No. 3).[26] In *Blackburn No. 1* Mr. Blackburn sought mandamus against the Metropolitan Police Commissioner to compel him to enforce certain gaming and betting laws. A confidential instruction had been issued by the Commissioner to senior officers of the London Metropolitan Police, containing a policy decision not to prosecute gambling clubs for breach of the gaming laws unless there were complaints of cheating or the clubs had become the haunts of criminals. In the court of first instance, Mr. Blackburn sought mandamus for three heads of relief. On appeal, he pursued only the third head — a reversal of the policy decision embodied in the special instruction. The Court of Appeal held that it was the duty of the Commissioner and also of chief constables to enforce the law; though chief officers of police have discretion — for example, whether to prosecute in a particular case — the court might interfere in respect of a policy decision amounting to a failure of the duty to enforce the law. The following statements of Lord Denning, M.R. are of interest:[27]

> I hold it to be the duty of the Commissioner of Police, as it is of every chief constable, to enforce the law of the land. He must take steps so as to post his men that crimes may be detected; and that honest citizens may go about their affairs in peace. He must decide whether or not suspected persons are to be prosecuted; and, if need be, bring the prosecution or see that it is brought; but in all of these things he is not the servant of anyone, save of the law itself. No Minister of the Crown can tell him that he must, or must not, keep observation on this place or that; or that he must, or must not, prosecute this man or that one. Nor can any police authority tell him so. The responsibility for law enforcement lies on him. He is answerable to the law and to the law alone.

---

[25] [1968] 1 All E.R. 763 (C.A.).

[26] [1973] 1 All E.R. 324 (C.A.).

[27] *Ibid.*, at p. 769.

> Although the chief officers of police are answerable to the law, there are many fields in which they have a discretion with which the law will not interfere. *For instance, it is for the Commissioner of Police, or the chief constable, as the case may be, to decide in any particular case whether enquiries should be pursued, or whether an arrest should be made, or a prosecution brought.* It must be for him to decide on the disposition of his force and the concentration of his resources on any particular crime or area. No court can or should give him direction on such a matter. He can also make policy decisions and give effect to them, as, for instance, was often done when prosecutions were not brought for attempted suicide; but there are some policy decisions with which, I think, the courts in a case can, if necessary, interfere. Suppose a chief constable were to issue a directive to his men that no person should be prosecuted for stealing any goods more than £100 in value. I should have thought that the court could countermand it. He would be failing in his duty to enforce the law. (Our emphasis.)

56. A similar issue arose in respect of police discretion in *Blackburn No. 3*. There Mr. Blackburn moved for an order of mandamus to direct the Commissioner to secure the enforcement of the law relating to obscene materials and to reverse the decision of the Commissioner that no police officers would be permitted to prosecute offenders against those laws without the prior consent of the Director of Public Prosecutions. The Court of Appeal held that, although the evidence disclosed that obscene material was widely available, the applicant had not established that it was a case for the court to interfere with the discretion of the police in carrying out their duties. Lord Denning, M.R. concluded that:[27]

> . . . the police have a discretion with which the courts will not interfere. There might, however, be extreme cases in which he was not carrying out his duty. And then we would. I do not think this is a case for our interference. In the past the commissioner has done what he could under the existing system and with the available manpower. The new commissioner is doing more. He is increasing the number of the Obscene Publications Squad to 18 and he is reforming it and its administration. No more can reasonably be expected.

57. From the foregoing principles and authorities, we draw the following two conclusions. First, generally, the decision in a given case to forbear in charging an offender where investigation is continuing in respect of other offences adjudged by the police as more serious, or in respect of other activities assessed to be a greater threat to Canada, is a proper exercise of a peace officer's discretion and will not constitute a breach of trust in connection with the duties of his office, provided that the discretion is exercised in good faith and for proper motives. Second, it will be otherwise where the forebearance amounts to a complete failure to enforce the law, as, for example, where a known trafficker in drugs is allowed indefinitely to continue in his crime with impunity, to the knowledge of the police. We are enquiring into certain instances in which it has been alleged to us that the R.C.M.P. has allowed a source who is a known trafficker in drugs to continue trafficking with impunity upon the condition

[28] *Ibid.*, at pp. 331-2.

that he provide information about others when asked. In a future report we shall consider those allegations in detail and make recommendations as to what the practice should properly be.

(ii) Section 383, Criminal Code of Canada

58. By virtue of section 383(1) of the Criminal Code of Canada, it is an offence "corruptly" to give any form of benefit to an agent or employee in exchange for that person doing any act or showing any favour in relation to the principal's or employer's affairs or business. The issue arises whether in those cases in which the R.C.M.P. has obtained information from a paid undercover operative who is also an employee or agent, and in which the information related to the principal's or the employer's business, the R.C.M.P. has committed the offence created by section 383(1).

59. Section 383 of the Code is entitled "Secret Commissions — Privity to Offence — Punishment — Definitions". It appears in Part VIII of the Code, which is entitled generally "Fraudulent Transactions Relating to Contracts and Trade". The section itself reads as follows:

> 383. (1) Every one commits an offence who
>
> (a) corruptly
>
> (i) gives, offers or agrees to give or offer to an agent, or
>
> (ii) being an agent, demands, accepts or offers or agrees to accept from any person,
>
> a reward, advantage or benefit of any kind as consideration for doing or forbearing to do, or for having done or forborne to do, any act relating to the affairs or business of his principal or for showing or forbearing to show favour or disfavour to any person with relation to the affairs or business of his principal...
>
> (2) Every one commits an offence who is knowingly privy to the commission of an offence under subsection (1).
>
> (3) A person who commits an offence under this section is guilty of an indictable offence and is liable to imprisonment for two years.
>
> (4) In this section "agent" includes an employee, and "principal" includes an employer.

The offences generally resemble those dealing with bribery of public officials created by sections 110 and 112 of the Code, and appear to be intended to discourage similar evils respecting private master-servant and principal-agent relationships.

60. In order for the offence to be committed, it need not be shown that the giving of the information or the act done by the agent was in any sense injurious to the principal's affairs, or even contrary to his best interests. It would appear that the interest sought to be protected is the integrity of the relationship itself, and that the gist of the offence is that a third party subverts that integrity by paying the agent to do an act affecting the relationship.

61. It is also noteworthy that the offence lies not in the performance of the act or the exercise of favour but rather in the corrupt offer of or demand for

reward. The act of the agent might itself be entirely proper, and indeed form part of the lawful duties which he is bound to perform. Nevertheless, an offence is committed if reward is given in consideration of the act or forbearance.

62. In part, the section codifies the common law with respect to the fiduciary obligations of agent and servant — specifically that they should receive no secret profit or benefit. The receipt of a reward or benefit, and perhaps the mere demand by the fiduciary for such an advantage, is a tortious breach of his duty. However, it cannot be any breach of duty on the part of the agent or employee if a third person offers him a secret advantage which he refuses, although the third person may be criminally liable pursuant to section 383(1) of the Code.

63. Sections of the Code which prohibit bribery of those in public positions refer only to the giving and accepting of benefits and rewards: the adverb "corruptly" does not appear, as it does in section 383(1). It would at first appear that the word "corruptly" contained in section 383(1) adds an element to the offence which would be lacking in the conduct of a police or security officer in bribing an agent to inform on his principal. The defence would rest upon the higher motive and lofty intent which inspired the bribe, the conduct amounting to anything but "corruption". That defence is not available, however, since there is clear and strong authority in Canada that the word "corruptly" does not add an element which must be proven to establish guilt; rather, the word is redundant, since the act which is prohibited by the section has been held to be intrinsically corrupt and so cannot be done under innocent or extenuating circumstances. Perhaps the clearest illustration of the judicial interpretation placed upon the section is afforded by *R.* v. *Brown*.[28] In that case, Mr. Justice Laidlaw, of the Ontario Court of Appeal, turned his attention to the purpose for which the section was enacted:

> The evil against which that provision in the Criminal Code is directed is secret transactions or dealings with a person in the position of agent concerning the affairs or business of the agent's principal. It is intended that no one shall make secret use of the agent's position and services by means of giving him any kind of consideration for them. The agent is prohibited from accepting or offering or agreeing to accept any consideration from anyone other than his principal for any service rendered with relation to the affairs or business of his principal. It is intended to protect the principal in the conduct of his affairs and business against persons who might make secret use, or attempt to make such use, of the services of the agent. He is to be free at all times and under all circumstances from such mischievous influence. Likewise, it is intended that the agent shall be protected against any person who is willing to make use secretly of his position and services... In my opinion, the act of doing the very thing which the statute forbids is a corrupt act within the meaning of the word "corruptly" used in the section under consideration. I think that word was

[29] The cases which have considered the section are *R.* v. *Gross*, [1946] O.R. 1; *R.* v. *Brown*, [1956] O.R. 944 and *R.* v. *Reid*, [1969] 1 O.R. 158, all of which are decisions of the Court of Appeal for Ontario.

> intended to designate the character of the act prohibited by the legislation. If a person were to give a sum of money, secretly, to an agent for the very purpose of having him do some act... it could not be said that he did not intend to contravene the provisions of section 368[383], or that he acted honestly or in good faith. It must be held that he intended to do the very thing Parliament intended to prohibit. His act can be regarded only as a corrupt act. In my opinion, it is not an answer in law for a person to say that he believed he had a right to have a certain thing done by an agent's principal, or that he believed that the agent ought to have done the act in question with relation to the affairs or business of his principal. His belief in respect of his rights does not justify his doing the very act intended to be prohibited by law.[30]

Mr. Justice Gibson, dissenting, would have concurred in the result on the evidence but differed on the meaning of the word "corruptly". He was unable to agree that a payment honestly made would be corrupt, merely because it amounted to the very act otherwise described in section 383. He referred to the common dictionary definition of "corrupt", and concluded that at the least, an act done "corruptly" is done with an evil mind — with evil intention, and except where there is an evil mind or intention accompanying the act, it is not done corruptly. He concluded:

> From the definitions it is difficult to understand how a corrupt act could be honestly performed.
>
> If the interpretation placed upon s.368[383] by the trial judge when he recalled the jury is correct the word "corruptly" in the section is superfluous, and any payment to an agent for doing or forbearing to do any act relating to the affairs or business of his principal is automatically an offence — whether such payment is made with honest intentions or dishonestly.
>
> This, in my opinion, goes beyond the true intent of the statute.[31]

64. The rationale underlying Mr. Justice Gibson's dissenting view in *Brown* was rejected by the English Court of Appeal in *R.* v. *Smith*.[32] There, the accused had offered a bribe to a public official. When charged, he raised the defence that he had done so with the altruistic intention of subsequently exposing the corrupt public servant. It was held that his ulterior motive was irrelevant. The accused acted "corruptly", as that word appeared in the statute, because he deliberately did an act — i.e. conferred a benefit upon a person in a defined class — which the statute forbade. In delivering the judgment of the Court, Lord Parker, Lord Chief Justice, concluded that the object of such legislation was to prevent public servants from being subjected to temptation. The very act of offering was prohibited, and the word "corruptly" added nothing to the Crown's burden in making out a case.

65. A second line of authority, emanating from English and Australian courts, attaches some significance to the word "corruptly". In an Australian case, *Rex* v. *Stevenson*,[33] Mr. Justice Hood considered the meaning of the word

[30] [1956] O.R. 944 at p. 946.
[31] *Ibid.*, at p. 962.
[32] [1960] 1 All E.R. 256.
[33] [1907] V.L.R. 475 at 476. (S.C. of Victoria).

"corruptly" in the Secret Commissions Prohibition Act, 1905 and concluded that in that Act, "corruptly" must mean some wrongful intention. In *C.* v. *Johnson*,[34] the Supreme Court of South Australia examined the meaning of the word "corruptly" in the Secret Commissions Prohibition Act, 1920. Mr. Justice Travers stated:

> On normal legal principles one would expect that word [corruptly] to add something to the meaning of the section... I think that this statute does import that the defendant was acting *mala fide*... and with wrongful intention...
>
> My view is that the commission of an offence against [the Act] necessarily involves dishonesty, and that a man who acts corruptly within the meaning of that section [of the Act] necessarily acts dishonestly.[35]

66. English decisions have also illustrated an inclination to attribute some meaning to the word "corruptly". Although Mr. Justice Willes in the 1858 decision in *Cooper* v. *Slade*[36] indicated that the word "corruptly" in an election statute did not mean "dishonestly", a number of subsequent cases have imported some notion of dishonesty when the word "corruptly" appeared. In *Bradford Election Petition — No. 2*,[37] Baron Martin stated that the word "corruptly" meant "an act done by a man knowing that what he does is wrong, and doing so with evil feelings and with intentions". More recently, in *R.* v. *Lindley*,[38] D Mr. Justice Pearce interpreted the word "corruptly" in the Prevention of Corruption Act, 1906 to require a dishonest intention. In *R.* v. *Calland*,[39] Mr. Justice Veale referred to *Lindley* and directed a jury considering that same Act that "corruptly" meant dishonestly. The *Calland* case, decided in 1967, may not, however, have taken into account the 1960 decision of the English Court of Appeal in *R.* v. *Smith*.[40]

67. It can be seen that the Australian courts have imported an element of dishonesty into the word "corruptly". English courts have wavered, but it is submitted that the Court of Appeal decision in *Smith* resolves the issue; the word "corruptly" imports no notion of dishonesty. The subsequent decision in the *Calland* case may be regarded as having been made *per incuriam*. In any event, the questions raised by the interpretation of "corruptly" have clearly been resolved in Canada. In Canada, the word "corruptly", at least as used in section 383, is redundant. We submit that this is the proper interpretation, since the very act of rewarding an agent or employee for doing something in connection with his principal's or employer's business violates the integrity of a relationship that is sought to be protected.

68. We pass to the question whether any defences are available to R.C.M.P. members who have paid agents to do an act or show favour with relation to

---

[34] [1967] S.A.S.R. 279 (S.C.).
[35] *Ibid.*, at p. 291.
[36] 6 H.L.C. 746 at 773.
[37] (1869), 19 L.T.R. 723 at 727.
[38] [1957] Crim. L.R. 321 (Lincolnshire Assizes).
[39] [1967] Crim. L.R. 236 (Lincolnshire Assizes).
[40] [1960] 2 Q.B. 423.

their principal's affairs. Where the principal or employer is engaged in crime, there is no lawful relationship the integrity of which is worthy of protection; no crime is committed should the agent or employee pass information for pay to the R.C.M.P. Although there are no cases which have considered this point, we do not interpret section 383(1) as protecting relationships tainted by a criminal object. Similarly, we consider that section 383(1) has no application where the information conveyed by the agent or employee, even when it affects the lawful affairs of his principal, provides evidence of a crime. The difficult issue in this context is whether section 383(1) is violated when the R.C.M.P. pays an agent or employee to report about the lawful business or affairs of his principal or employer, and no evidence of a crime is produced thereby. There have been circumstances in which the R.C.M.P. (and particularly the Security Service) have solicited and received such information in relation to its role in gathering intelligence. Is an offence thereby committed? If so, are there defences available?

69. We first consider motive. It may be argued that the act was performed with a higher purpose in mind. Courts in Canada, Britain and the United States have repeatedly held that "the criminal nature of an act is not purged by good motive...".[41] Glanville Williams cites the Criminal Law Commissioner's 7th Report (1843):

> To allow any man to substitute for law his own notions of right, would be in effect to subvert the law.

Even in the United States, where certain punitive provisions have been held not to apply to police officers executing their duties, altruistic intention or motive is no defence to crime.[42] A crime is a crime although committed for the ultimate purpose of enforcing the law.[43] This issue is dealt with more fully in Part IV.

70. Similarly, we consider that defences are not afforded upon the principles of Crown immunity or public policy; nor do we feel section 25 of the Criminal Code provides an answer to such a charge. The common law defence of necessity is also not available in such circumstances, as the practice of paying secret commissions is merely one of a variety available to the Force to gather information about a given subject. It cannot be said to be a "necessary" technique, although it is undoubtedly an effective one. These issues are also discussed in detail in Part IV.

71. Thus, there may have been violations of section 383 of the Criminal Code where the R.C.M.P. has given, or has offered or agreed to give a reward, advantage or benefit to an agent or employee of a principal or employer, in consideration of that person furnishing information concerning the business or affairs of his principal or employer, unless that information was evidence of the commission of a crime.

---

[41] Glanville Williams, *Criminal Law: The General Part*, 2nd ed., London, Stevens, 1961, at 748.

[42] *People* v. *Williams*, (1952) 113 N.Y.S. (2d) 167.

[43] *Hamp* v. *State of Wyoming*, 118 P. 653. See generally *Corpus Juris Secundum*, Criminal Law, Vol. I, pp. 9ff.

72. If the law does make the furnishing of such information an offence, the consequences from the point of view of the gathering of criminal intelligence (which may not provide evidence of a crime or of an unlawful business activity) by any police force — not just the R.C.M.P. — are seriously adverse to effectiveness, if the police force is expected to remain within the law. Similarly, the consequences from the point of view of the effectiveness of Canada's security intelligence agency are serious, if the agency is to be expected to use only lawful techniques. It would render impossible making payments to certain sources engaged in a counter-espionage investigation or paying a source who has penetrated a subversive organization and is in its employ in exchange for information about the affairs of the organization.

73. In the absence of further interpretation of section 383, it is not possible to define the limits of permissible police and intelligence behaviour beyond the limits of reasonable conjecture. This ambiguity is addressed and we make recommendations on the matter in Part V, Chapter 4 and Part X, Chapter 5.

(iii) Statutory barriers to obtaining information from sources with access to "private sector" records

74. By the expression "access to private sector records" we mean the obtaining, from a source who is not in the employ of a government institution, information which he possesses by reason either of a business or professional relationship with a third party. For example, a lawyer or doctor in private practice may have records or personal knowledge of discussions with clients or patients who may be of interest to a security intelligence agency or a police force. A manager of a financial institution (e.g. a bank or trust company) might also have access to financial data concerning individuals of interest.

75. Although we have heard no evidence concerning instances of R.C.M.P. access to private sector records, we have examined the R.C.M.P. submission to the Commission of Inquiry into the Confidentiality of Health Records in Ontario in June 1979. That submission identified a number of situations when the R.C.M.P. had approached private medical practitioners in order to obtain medical or biographical information. In the area of V.I.P. security, the submission noted that the R.C.M.P. had approached doctors some 147 times within the past 15 years in order to determine whether a given individual constituted a threat to the safety of a V.I.P. The R.C.M.P. has also, although less frequently, approached medical doctors and psychiatrists about the reliability of individuals, for security screening purposes. The submission noted that on two occasions R.C.M.P. officers approached medical doctors for information on prescriptions given to patients, in order to further drug investigations.

76. We have no data on the number of occasions, if any, on which the R.C.M.P. has approached other professionals to act as sources in providing access to private sector records, and therefore we cannot treat approaches to these other professionals as "past practices not authorized or provided for by law". Nonetheless, we raise the possibility of the violation of federal and provincial laws in obtaining access to private sector records because of the

potential problems to be encountered in this area. Similar problems have surfaced in the United States.

77. Federal restrictions on the use of sources with access to private sector records are few. One statute, the Telegraphs Act,[44] requires certain employees of private telegraph companies falling under federal jurisdiction to swear an oath of secrecy as to information they acquire in the course of their duties. Unauthorized disclosure is a summary conviction offence. Another example of federal controls on private sector information is the Canada Shipping Act,[45] which provides for the privacy and confidentiality of wireless messages sent to ships at sea. The penalty for wrongful disclosure may include a fine and imprisonment.

78. More likely to constitute barriers are provincial statutory restrictions on the disclosure of personal information obtained in the course of a professional or commercial relationship. We have reviewed provincial legislation governing the legal and medical professions in Quebec and Ontario as examples of such statutory provisions. These provisions serve as a general illustration of restrictions likely to be found in other provinces. In both Ontario and Quebec, the legislation we examined sets up a framework, *inter alia*, for regulating the conduct of professionals through a governing body.

79. In Ontario the Health Disciplines Act[46] and the regulations enacted pursuant to it define as professional misconduct a breach by a medical doctor of his obligation of confidentiality vis-à-vis his patients. Such conduct is punishable by a variety of disciplinary sanctions administered by the governing body. Exceptions to the general rule of confidentiality are very narrow and would not extend to most security intelligence agency or criminal investigations, nor would they permit release of a patient's psychiatric or medical files to enable authorities to cope with an emergency such as a terrorist attack or a hostage-taking incident. The severity of the confidentiality rule is mitigated by the fact not only that the disclosure must come to the attention of the Discipline Committee but that when it does the Committee is unlikely to discipline a doctor if the disclosure were made to avert a threat to human life.

80. The Law Society Act[47] of Ontario and the regulations and rules enacted pursuant to it make it a breach of that profession's code of professional conduct to disclose, except in limited circumstances, confidential information concerning a client. Breach of the code of conduct by a lawyer may result in disciplinary sanctions, including the loss of professional status.

81. In Quebec, lawyers, notaries and medical doctors fall under the authority of the Code des Professions,[48] as do some 35 other professional bodies, such as pharmacists, social workers and chartered accountants. Section 87 of the Code requires that the "bureau" of each professional corporation adopt in regula-

---

[44] R.S.C. 1970, ch.T-3.
[45] R.S.C. 1970, ch.S-9.
[46] S.O. 1974, ch.47.
[47] R.S.O. 1970, ch.238.
[48] 1978 L.R.Q., ch.C-26.

tions a Code of ethics which must include confidentiality provisions. The code also establishes disciplinary procedures, including the creation within each professional corporation of a discipline committee which handles all complaints lodged against its members for violations of codes of ethics. For example, a violation of the Règlement concernant le code de déontologie[49] adopted by the medical profession may result in disciplinary proceedings against doctors who divulge confidential information. Likewise, the Règlement concernant le code de déontologie,[50] adopted by the Bar, and the Loi sur le Notariat[51] impose confidentiality requirements for lawyers and notaries respectively. Finally, the Quebec Charter of Human Rights and Freedoms[52] makes provisions for professional secrecy, and provides only narrow exceptions, which again would not extend to police or security intelligence investigations. The Charter provides in section 49 that any unlawful interference with any right or freedom recognized by the Charter entitles the victim to obtain cessation of such interference and compensation for the moral or material prejudice resulting therefrom. In the case of an unlawful and intentional interference, the party guilty of the interference may be condemned to pay exemplary damages.

82. While we do not wish to forecast the application of the secrecy provisions in Quebec, we are concerned that professionals who act as sources in providing access to private sector records may risk discipline, fines and the possible loss of professional status. This of course is primarily a problem for the source himself, but R.C.M.P. members who conspire with the source to effect an unlawful purpose may be guilty as a party to the offence by virtue of abetting it (section 21) and of the Criminal Code offence of conspiracy (section 423(2)).

83. In addition to the specific statutory provisions governing various professions, examples of which we have seen in Ontario and Quebec, general statutory or regulatory restrictions at the provincial level may govern disclosure of information to disinterested third parties. One such example is the Ontario Consumer Reporting Act.[53] That Act seeks to regulate the collection and dissemination of consumer credit information. Its provisions would restrict the release of personal, financial and career information to a security intelligence agency or police force, although identifying information (name, address, place of employment) may be released. This Act penalizes both the source who improperly provides access to private sector records and the person who seeks to obtain the information. Members of the R.C.M.P. who conspire with the source to breach the confidentiality provisions may again be liable to criminal charges of conspiracy under section 423(2) of the Code or, if the offence is committed, may be a party to the offence by virtue of having abetted it (section 21).

---

[49] Reg. 816-80, 20 mai 1980.
[50] Reg. 77-250, 5 mai 1977.
[51] L.R.Q. 1978, ch.N-2.
[52] S.Q. 1975, ch.6.
[53] S.O. 1973, ch.97.

in Canada to "turn" — i.e. to defect, or to remain in place as an agent of the Canadian Security Service — the member would thereby be guilty of an offence under section 63 of the Criminal Code. That section provides as follows:

> 63. (1) Every one who wilfully
>
> (a) interferes with, impairs or influences the loyalty or discipline of a member of a force,
>
> (b) publishes, edits, issues, circulates or distributes a writing that advises, counsels or urges insubordination, disloyalty, mutiny or refusal of duty by a member of a force, or
>
> (c) advises, counsels, urges or in any manner causes insubordination, disloyalty, mutiny or refusal of duty by a member of a force,
>
> is guilty of an indictable offence and is liable to imprisonment for five years.
>
> (2) In this section, "member of a force" means a member of
>
> (a) the Canadian Forces, or
>
> (b) the naval, army or air forces of a state other than Canada that are lawfully present in Canada.[54]

The section was introduced into Canada in 1953, one year after the passage of the Visiting Forces (British Commonwealth) Act and the Visiting Forces (North Atlantic Treaty) Act.[55] It may be inferred that the Parliamentary intent was to provide the same penalty for subversion of such forces as was applicable to subversion of members of the Canadian Forces. Whether that is a necessary inference or not, it is noted that the section defines "member of a force" as "a member of... forces of a state... that are lawfully present in Canada". While a military attaché may be lawfully present in Canada, he cannot be said to be a member of "forces" present in Canada. If the military intelligence officer is not a military attaché but is disguised in some non-military capacity in order to spy, he is not in Canada as "a member of a force" and, even though he holds a diplomatic visa, he may not be "lawfully" in Canada if he is engaged in espionage. Alternatively, whether the military intelligence officer is an attaché or described as a chauffeur, the fact that he holds a diplomatic visa is probably conclusive that he is present in Canada as a diplomat and not as a member of a military force. For these reasons, we conclude that the factual situation envisaged does not give rise to the commission of an offence under section 63.

(f) *Removal of property of others and its delivery to the police*

85. Undercover operatives, as well as supplying intelligence as a result of their personal observations, have removed documents of intelligence interest from a targetted organization. The classic example is that of Mr. Igor

[54] 1953-54, ch.51, s.63.

[55] S.C. 1952, chs.283 and 289.

Gouzenko who, in September 1945, defected from the Soviet Embassy in Ottawa with documentary evidence of Soviet espionage in Canada and the United States. Based on what Mr. Gouzenko told the police, the documents he brought with him and subsequent investigations, the R.C.M.P. pieced together the espionage roles of some officials of the Soviet Embassy and a number of other individuals. Yet witnesses before us have asked whether the removal of documents in circumstances such as Mr. Gouzenko's may amount to the offence of theft, contrary to section 283 of the Criminal Code, and whether the receipt and retention of documents by the Security Service may constitute the offence of possession of property obtained by crime, contrary to section 312 (1). We do not intend to quote those sections, for we consider that the law of theft and of possession of stolen property does not impede the receipt and retention of documents defectors are likely to bring with them and which relate to the statutory mandate which we shall be recommending for the security intelligence agency. Any such documents are likely to relate to the commission of crime, and in our view the removal and retention of such documents by the defector or members of the security intelligence agency would not be a crime, if the information is disclosed to the appropriate law enforcement authority.

86. We recognize that there may be cases in which a defector brings documents to the security intelligence agency and those documents are neither evidence of a crime nor do their contents fall within the purview of the agency's mandate. We do not consider that such a situation requires any change in the law. Rather, we think that it should be handled in accordance with the proposals which we have developed with respect to the dealings between the federal and provincial attorneys general when evidence that violations of the law, may have been committed by a member or agent of the security intelligence agency. Our proposal in that regard is found in Part V, Chapter 8.

(g) *Civil wrongs*

87. A further issue of concern in both the Security Service and the C.I.B. is the commission of intentional civil wrongs by undercover operatives. While not involving a violation of federal, provincial or municipal law, civil wrongs merit consideration as an issue since they constitute an interference with personal rights to which society attaches significance and which the common and civil law therefore consider worthy of protection.

88. The range of potential civil wrongs arising from the use of undercover operatives is both broad and difficult to predict. Two acts in particular — inducing breach of contract and invasion of privacy — have been brought to our attention. We deal with these here.

89. The Force may have sought to obtain information from individuals such as bank managers whose positions impose upon them an express or implied duty in contract to keep in confidence information which they receive in that position. In such cases, the individuals may be civilly liable for breach of contract. R.C.M.P. members who procure such breaches of contract may be liable in tort for inducing breach of contract. One textbook states that liability for interference with contractual relations of this sort will attach if the intervenor

with knowledge of the contract and intent to prevent or hinder its performance, either,

(1) persuades, induces or procures one of the contracting parties not to perform his obligations, or

(2) commits some act, wrongful in itself, which prevents such performance.[56]

There appear to be two principal means in the situation noted above by which liability for inducing breach of contract may have been avoided. A leading text states:

> A distinction is sometimes drawn between persuasion, inducement or procurement, on the one hand, and advice on the other: the former being actionable, but not the latter...[57]

No liability attaches for simply advising an individual to breach his contract. It seems unlikely, however, that the means employed by the Security Service to "persuade" a person to breach his contract would be viewed as mere "advice".

90. The second and more likely means of avoiding liability for inducing breach of contract lies in the defence of justification. The same text notes:

> While spite or an improper motive on the part of the defendant is not an essential part of the plaintiff's cause of action, the purpose prompting his conduct may, on the other hand, be so meritorious as to require sacrifice of the plaintiff's claim to freedom from interference... The issue in each case being... whether, upon a consideration of the relative significance of all the factors involved, the defendant's conduct should be tolerated despite its detrimental effect on the interests of the other. For this purpose, it has been said, the most relevant are the nature of the contract, the position of the parties to it, grounds for the breach, the means employed to procure it, the relation of the person procuring it to the contract-breaker, and the object of the person procuring the breach. Thus, it seems clear that if the methods of interference are in themselves unlawful, at any rate where a fraud or physical violence is employed, there can be no justification, even if the defendant would have been privileged to accomplish the same results by proper means....
>
> In several cases, a privilege to protect the public interest has been recognized, as where the defendant acted for the sake of upholding public morality.[58]

While the Security Service (and indeed, the C.I.B., where such potential liability arises in the course of its undercover operations) may not be protecting public morality, there is a compelling argument that inducing an individual to provide information for intelligence reasons in breach of his contract can be justified on grounds of public interest.

---

[56] Fleming, *The Law of Torts*, Sydney, The Law Book Company, 1977, (5th ed.), at p. 678.

[57] *Ibid.*, at p. 679.

[58] *Ibid.*, at pp. 682-3.

91. The second possible civil wrong we examine here is that which the same textbook states

> . . . is often compendiously called the 'right of privacy'. In its broadest sense, the interest involved is that of 'being left alone', of sheltering one's private life from the degrading effects of intrusion or exposure to public view.[59]

The text notes that the right to privacy has not, at least under that name, received explicit recognition by British courts. Another text also lists infringement of privacy as a "doubtful tort".

> The balance of such authority as there is, appears to be clearly against the existence of any independent tort of invasion of privacy...[60]

It is not clear in Canada whether an independent tort of invasion of privacy exists. In *Motherwell* v. *Motherwell*[61] the plaintiff succeeded in an action for breach of the right of privacy. In *Burnett* v. *The Queen in Right of Canada*,[62] the court held that it is not clear that there is no tort of invasion of privacy so that the action must proceed to trial on its merits. The court quoted from an earlier decision where it was said:

> It may be that the action is novel, but it has not been shown to me that the Court in this jurisdiction would not recognize a right of privacy. The plaintiff therefore has the right to be heard, to have the issue decided after trial.[63]

92. In the absence of a clear statement as to whether invasion of privacy is a tort, so that protection of the right of privacy is afforded as it is by privacy legislation enacted in some provinces, we must consider other bases for the potential right of action. The tort of trespass would not afford such a basis, since its boundaries are defined in relation to the plaintiff's person and property, and are not drawn in relation to a broader right to be left alone. Even the tort of nuisance offers only modest support; for the tort to occur, the offensive conduct must be devoid of any social utility and directed solely at causing annoyance. It is unlikely that the use of undercover operatives for a legitimate criminal investigative purpose or in order to fulfill the mandate of the Security Service can be regarded as an activity devoid of social utility. Therefore, in light of the uncertainty surrounding the existence or scope of the tort of invasion of privacy, and the probable inapplicability of trespass and nuisance to typical undercover operatives, we do not consider that these torts pose a real legal problem in undercover operations, at least so long as such operations are carried out within the mandate of the respective branches of the Force.

---

[59] *Ibid.*, p. 590.
[60] *Winfield and Jolowicz on Tort*, (10th ed.), at p. 492.
[61] (1976) 3 D.L.R. (3d) 62 (Alta. C.A.).
[62] (1979) 23 O.R. (2d) 109 (Ont. H.C.).
[63] *Krouse* v. *Chrysler of Canada* [1970] 3 O.R. 135 at 136.

C. NEED AND RECOMMENDATIONS — BRIEF SUMMARY

93. There can be no doubt about the continued need to use undercover operatives both for criminal investigation and security intelligence work. When information is required about those who maintain a high degree of secrecy in carrying out criminal activities or activities threatening the security of Canada, often the use of undercover operatives is the only effective means of obtaining it. However, as our analysis of the legal difficulties involved in the use of undercover operatives has shown, very serious doubt exists as to whether operatives may be used by either the criminal investigation side or the security intelligence side of the R.C.M.P. without violating existing federal and provincial laws. Therefore, because we think the use of undercover operatives is necessary and because we believe that both police and security intelligence practices should be lawful, we will recommend a number of changes in the law to remove doubts about the reasonable use of operatives for both police and security purposes. We will make our detailed recommendations for changes relating to security intelligence operations in Part V, Chapter 4 and for changes relating to criminal investigations in Part X, Chapter 5.

94. One other legal issue which may arise in using undercover operatives is entrapment. Entrapment arises as a legal issue only in cases resulting in prosecution. Therefore, it will be dealt with primarily as a problem relating to the criminal investigations side of the Force. Although there is no offence of entrapment in the Criminal Code, many believe (a) that such an offence should be introduced into the Code, or (b) that a defence should be established for an accused person who committed a criminal act as a result of inducement by an undercover operative, or (c) that evidence obtained by entrapment should be excluded, or (d) some combination of the above. We will make our recommendations on this subject in Part X, Chapter 5.

CHAPTER 10

INTERROGATION OF SUSPECTS — C.I.B. AND SECURITY SERVICE

A. CRIMINAL INVESTIGATIONS

1. Much of the work of the police consists of asking questions of innocent people as well as suspects. The Supreme Court of Canada has recognized the crucial role that is played by police questions in the investigation of crime. In *R.* v. *Fitton*[1] it was said that "it would be quite impossible to discover the facts of a crime without asking questions of persons from whom it was thought that useful information might be obtained". The law on police interrogation of suspects is almost entirely the result of judicial decisions as to the admissibility in evidence of statements made by suspects to police officers. Some principal features of this judge-made law will be referred to in this chapter.

2. The present R.C.M.P. Operational Manual begins with a foreword by Commissioner Simmonds dated September 1, 1977. It includes the following paragraph:

> Each member shall observe and comply with the policy and procedural directives in this manual, and is expected to interpret them reasonably and intelligently in the best interests of the Force.

The chapter entitled "Interrogations and Statements" has stated the following policy since September 12, 1979:

> A member must avoid unethical conduct of any type when he interrogates a person, e.g., causing mental or physical suffering, and must pay particular attention to the provisions of the Canadian Bill of Rights.

The policy has been the same, at least since December 1, 1978, except that there had been no reference to the Canadian Bill of Rights.

3. Assuming that the paragraph quoted from the Commissioner's foreword constitutes a "standing order", a breach of that policy might constitute a "minor service offence" under section 26 of the R.C.M.P. Act. If the conduct were so grave as to be "scandalous" or "disgraceful" or "immoral" it might constitute a "major service offence" under section 25 of the Act. Consequently we are within paragraph (a) of our terms of reference in considering whether any features of interrogation and taking statements from suspects would be "unethical", for such conduct would be conduct "not authorized or provided

[1] (1956) 116 C.C.C. 1 at 30.

for by law". We shall consider these features here, and in Part X, Chapter 5 we shall make recommendations arising from our findings. However, as our terms of reference, as far as criminal investigations are concerned, do not permit us to inquire into or make recommendations on a broad scale concerning the law or the practice governing the R.C.M.P. in criminal investigations, we shall limit our remarks and recommendations to those relating to and arising from conduct that may be "not authorized or provided for by law". It follows that we do not intend to discuss some of the proposals that have been made for radical revision of the present law.

4. Before we embark on an examination of interrogation techniques it is important to underline that the police do not have a general power to detain persons for questioning. As Lord Devlin has said:

> The police have no power to detain anyone unless they charge him with a specified crime and arrest him accordingly. Arrest and imprisonment are in law the same thing. Any form of physical restraint is an arrest and imprisonment is only a continuing arrest. If an arrest is unjustified, it is wrongful in law and is known as false imprisonment. The police have no power whatever to detain anyone on suspicion or for the purpose of questioning him. They cannot even compel anyone whom they do not arrest to come to the police station. It is true that in the course of an inquiry they frequently ask people to come to the police station and make a statement there and that people almost invariably comply.[2]

Thus, the legal right to interrogate arises only after there has been an arrest, although, as pointed out by Lord Devlin, questioning often occurs in the absence of an arrest.

5. Of all criminal investigation techniques, this power of the police to question persons suspected of crime is the one most often suspected by the public of being open to abuse. On the other hand, the manner in which accused are questioned is frequently open to review by the courts, which have reserved a right to reject statements made by an accused person to the police. There have been no indications, whether by complaint to us or examination of the files of the R.C.M.P., that in the manner in which members of the R.C.M.P. question suspects and take statements there is a general pattern of conduct which is contrary to law or even subject to criticism on ethical grounds. Nevertheless, there are some disquieting facts which have come to light, and which indicate some degree of conduct which is not authorized or provided for by law and therefore requires comment by us.

The Roberts booklet

6. In 1975, questions in the House of Commons by Mr. David MacDonald, M.P., revealed that a document was in use by the Training and Development Branch of the R.C.M.P., entitled "Interrogation Techniques", written by Chief Inspector A.R. Roberts of the Calgary City Police. At the time the R.C.M.P.

---

[2] P. Devlin, "The Criminal Prosecution in England" (1960) at p. 68, quoted in Ed Ratushny, *Self-Incrimination in the Canadian Criminal Process*, Toronto, Carswell, 1979, p. 143.

confirmed, in a press release, that it was used in a course offered to senior investigators with between 5 and 15 years of experience. Mr. MacDonald characterized the techniques that were described in the document as "intimidation, manipulation and brain washing".[3] The Solicitor General of the time, the Honourable Warren Allmand, wrote to Mr. MacDonald on April 11, 1975, stating:

> . . . the booklet in itself does not represent Force policy on the subject. I feel that the Royal Canadian Mounted Police policy on interrogation is clear and is based largely on the Judges' Rules dealing with the admissibility of evidence. I am sure that you will be interested in reviewing the Judges' Rules and am attaching a copy for your information.

In the House of Commons Standing Committee on Justice and Legal Affairs, Mr. Allmand stated that the booklet had been used to stimulate discussion as to "the good and bad way of doing things", and that the author was brought in as a guest lecturer, but not because the Force was recommending the use of all the techniques listed, any more than bringing in an outside lecturer on Nazism or Communism meant that the Force was recommending those doctrines. He emphasized that the Force policy on interrogation is in the Operations Manual. The Deputy Commissioner, R.J. Ross, assured the Committee that

> in future in any such course of this nature there will be a final wrap-up, stating exactly. . . that the policy is such, and that we will not allow any deviation from the policy of the Force in this aspect.[4]

We are concerned that notwithstanding what was said orally nothing in the Operations Manual tells the recruit or the experienced investigator which of the many techniques listed by Chief Inspector Roberts are ethical and which are unethical and not permissible.

7. The booklet was used as a handout by Chief Inspector Roberts in late 1973 and supplied to candidates in two R.C.M.P. centralized training courses — the Investigational Techniques Course and the Drug Investigational Techniques Course. On June 4, 1975, the officer in charge of Training and Development advised all Commanding Officers that Chief Inspector Roberts' booklet "is no longer distributed on centralized training courses, due to the recent controversy". Since March 1979 a much shorter manual entitled "Interrogation" has been distributed to members attending courses that deal with the subject of interrogation, for example, Junior Constables (1 1/2-3 years of experience) and Senior Investigators (7-12 years). This manual deletes most of the objectionable material previously included in the Roberts booklet, but we note with concern the following advice contained in it:

> Make it difficult for the suspect to deny the crime by asking questions where he has two answers — both incriminating.

Examples are then given, and the text continues: "This type of question is most effective at crucial moments." The R.C.M.P. have advised us that "the manual

---

[3] House of Commons, *Debates*, March 26, 1975, p. 4531.

[4] Minutes, House of Commons Standing Committee on Justice and Legal Affairs, May 15, 1975, p. 26:19.

was developed by our Force Polygraphists". We hope that this extract does not represent the standards of polygraphic tests as used by R.C.M.P. polygraphers.

8. During June 1975 and afterwards no instruction was issued within the R.C.M.P. that the Roberts handbook was not acceptable. In 1980 the R.C.M.P. advised us that in view of the fact that "most, if not all the techniques described in it can be found in books generally available on the shelves of most libraries", no instructions were issued to members regarding the methods recommended. It is therefore not surprising to us that in the summer of 1980 our researcher was told by one officer, who had been trained in interrogation when the Roberts booklet was in use, that he learned only some considerable time after 1975 that many of the techniques there advocated are now frowned upon. Moreover, he was never so advised formally, as there has never been a directive as to what parts of the Roberts booklet are acceptable and what parts are not. It cannot be said that a press release stating that the booklet did not represent Force policy, without further comment for the benefit of investigators across Canada, can be taken as a serious internal criticism of those techniques.

9. Our review of the cases which have come to our attention reveals that there are four areas of interrogation which give rise to concern: the right to counsel, oppressive conduct, brutality, and trickery. In this chapter we shall discuss each of these in turn, with reference to the problems they have caused in the past, reserving our recommendations for change for Part V, Chapter 6 as they relate to the Security Service and Part X, Chapter 5 as they apply to criminal investigations.

The right to counsel

10. There are two aspects of this concern which require comment: whether members of the R.C.M.P. advise persons in custody of their right to counsel and whether persons in custody are denied counsel. There is no express requirement in Canadian law that a person under arrest be advised of his right to retain counsel. In comparison, section 29(2) of the Criminal Code imposes a duty upon everyone who arrests a person "to give notice to that person, where it is feasible to do so, of... the reason for the arrest". It is true that section 2(c)(ii) of the Canadian Bill of Rights recognizes the right of "a person who has been arrested or detained" to "retain and instruct counsel without delay", but it says nothing as to whether he must be advised that he has that right. The R.C.M.P. Operations Manual states:

> Advise prisoners of their right to engage legal counsel or to get advice from a relative or friend.

This requirement probably goes beyond the requirements of the Canadian Bill of Rights, and for this the R.C.M.P. is to be commended. On the other hand, there is some uncertainty as to the scope of application of the instruction, for it is unclear who are to be regarded as "prisoners" for this purpose. The chapter in the Operational Manual on interrogation makes no reference to this directive. We infer from this that it is not intended to be applied to persons being interrogated. Indeed, the silence in both the chapter on interrogation and

the chapter on arrest, on the subject of advising of the right to engage counsel may indicate that the Force does not require its members to advise persons who are being questioned but not yet arrested, or persons arrested but not yet charged, to be advised of their right to counsel. Moreover, we have been advised by senior officers of the R.C.M.P. that there is no Force policy requiring persons who are not in custody to be advised of their right to counsel.

11. There may be circumstances in which the right to contact a lawyer, and to be advised of that right, should be tempered. The English Judges' Rules (which are not the law in England or in Canada, but are considered good practice in both countries and are published in the R.C.M.P. Operational Manual), have appended to them administrative directions (not published in the R.C.M.P. manual) which, in this regard, face up to interests which compete in certain circumstances. Under the heading of "Facilities for Defence" they say:

> a person in custody should be allowed to speak on the telephone to his solicitor or to his friends, provided that no hindrance is reasonably likely to be caused to the processes of investigation, or the administration of justice by his doing so.

The proviso is intended to entitle the police to refuse a person in custody the right to contact his lawyer (or friends) when there is reason to think that his doing so may hinder the investigation underway by tipping off other suspects not yet in custody. We doubt that this proviso, however reasonable, is consistent with the provision in the Canadian Bill of Rights. An allegation made to us, with respect to which we shall be reporting in detail in another Report, illustrates the problem. R.C.M.P. officers from a certain detachment, together with other R.C.M.P. and municipal officers, arrested a number of people on drug-related charges. The arrested persons were first taken to the detachment cells. One of the accused was allowed, by a constable acting on his own initiative, to telephone his wife to ask her to come to the police station to pick up their three-year old child who had been with the father at the time of his arrest. Later, during that afternoon, the R.C.M.P. corporal in charge of the investigation, who had been made aware that the earlier call had been made, allowed the same accused to speak on the telephone to his lawyer. Apart from these two calls, the remainder of the investigation was typified by attempts by the police to prevent the arrested persons from making telephone calls and to prevent lawyers, who were attempting to contact clients, from being able to do so. After a defence lawyer involved in the case wrote to us about the experience, the R.C.M.P. conducted an internal investigation. It produced the following results:

(a) Members of the squads who had been involved in the events, and detachment personnel who were present at the station, when asked by lawyers, claimed either not to know where the prisoners were or that they did not know which other detachment the prisoners had been taken to.

(b) Lawyers were told that the officer in charge of the case would be informed of their request or that inquiries would be made to obtain the necessary information, but nothing was done in furtherance of these assurances.

(c) Official forms which ought to have identified who had arrested whom and where the persons detained were lodged were not completed properly. On four of the forms, notations expressly stated that no telephone calls were to be permitted to the prisoners concerned. The identity of the persons who wrote those notations could not be traced.

(d) One of the accused was moved from the original cells to R.C.M.P. cells at another detachment, then back to the original cells, then to still another detachment, then back to the original cells again, and finally to the provincial correctional facility, all in the course of three days and three hours.

(e) Officers involved in the case gave, as reasons for the various movements of prisoners, "lack of room" in the original detachment, "security", "separation of the accused", "investigational purposes".

(f) The original purpose of the "no telephone calls" order may well have been to prevent prisoners from hindering the continuing investigation by informing co-conspirators of what was happening. However, many of the officers involved evidently translated this purpose into a practice of not allowing the persons detained to have access to counsel, for reasons that were unrelated to the original purpose.

12. Judicial consideration of the admissibility of statements made by suspects is, as it relates to the right to counsel, an insufficient incentive to the attainment of proper standards. It has been held that even a specific denial by the police to allow an accused to contact his lawyer, despite the contravention of the Canadian Bill of Rights, will not render a statement thereafter obtained from him inadmissible on that account.[5] This judicial attitude has led the R.C.M.P. in at least one training course in 1972, to present the following examination question: "The accused, Mr. O'Connor, was refused permission to obtain counsel by the police at the police station. Is this illegal?" The desired answer was "No, it was not illegal". In another case, a retrial was ordered because of a denial of counsel, but the most that can be said is that this will be an important factor when a court decides whether or not a statement is voluntary.[6] No case stands for the proposition that a statement obtained after a denial of counsel must be held to be inadmissible. Although one judge has expressed the view that denial of counsel by police may give rise to a civil action in tort or possibly criminal action (for disobeying a federal statute, under section 115 of the Criminal Code), the Canadian Committee on Corrections has argued to the contrary:

> Section 2(c)(ii) of the Canadian Bill of Rights does not command a police officer to do anything. It is a direction to a court not to construe the law of

---

[5] *R.* v. *Steeves* [1964] 1 C.C.C. 266 (N.S.C.A.). See also, *O'Connor* v. *R.* [1966] 4 C.C.C. 342 (Sup. Ct. Can.) and *Hogan* v. *The Queen* (1974) 48 D.L.R. (3d) 427 (Sup. Ct. Can.).

[6] *R.* v. *Ballegeer* [1968] 66 W.W.R. 570 (Man. C.A.).

arrest in such a way as to infringe the right of a person who has been arrested to retain a lawyer.[7]

Oppressive conduct

13. As already stated, Canadian courts will not admit a statement made by an accused person unless the prosecution proves that the statement was made voluntarily. In one of the most recent judgments in the Supreme Court of Canada, *Horvath* v. *The Queen*, Mr. Justice Martland said:

> . . . to render a statement of the accused to a police officer inadmissible there must be the compulsion of apprehension of prejudice or the inducement of hope of advantage whether that apprehension or hope be instigated, induced or coerced.[8]

He reconfirmed that, as had been held in an earlier case in the Supreme Court of Canada, the primary question is whether the statement was made voluntarily in the sense that it has not been obtained from the accused either by fear of prejudice or hope of advantage exercised or held out by a person in authority. Mr. Justice Martland declined to consider whether, beyond those circumstances, facts which constitute "oppression" would result in a statement being ruled inadmissible. It is true that Mr. Justice Martland's judgment, with which two other members of the Court agreed, was one which dissented in the result of the case, and, as will be seen, his statement of the law represents the narrowest of the statements of the concept of voluntariness found in the *Horvath* case. In England, it has been held that "oppressive questioning" will result in the exclusion of a statement, oppressive questioning being defined as "questioning which by its nature, duration or other attendant circumstances (including the fact of custody) excites hopes (such as the hope of release) or fears, or so affects the mind of the suspect that his will crumbles and he speaks when otherwise he would have remained silent".[9] In *Horvath* v. *The Queen*, Mr. Justice Beetz, who spoke for himself and one other member of the Court, said that the principle of voluntariness may extend

> to situations where involuntariness has been caused otherwise than by promises, threats, hope or fear, if it is felt that other causes are as coercive as promises or threats, hope or fear, and serious enough to bring the principle into play.[10]

The third judgment in that case was delivered by Mr. Justice Spence, with whom one other judge agreed. He also expressed the view

> that a statement may well be held not to be voluntary. . . if it has been induced by some other motive or for some other reason than hope or fear.[11]

---

[7] *Report of the Canadian Committee on Corrections, Toward Unity: Criminal Justice and Corrections*, 1969, p. 143 note 23. The judge referred to was Mr. Justice Coffin in *R.* v. *Steeves*.

[8] [1979] 2 S.C.R. 376 at 388. See also *Ward* v. *The Queen* [1979] 2 S.C.R. 30.

[9] *The Queen* v. *Prager* [1972] 1 All E.R. 1114 (C.A.).

[10] [1979] 2 S.C.R. 376 at 424-5.

[11] *Ibid.*, at 401.

He found that in the circumstances of that case the accused's statements had been made at a time when he was suffering from "complete emotional disintegration", and that "no statement made by that accused under those circumstances can be imagined to be voluntary".

14. These recent judicial statements indicate that the precise bounds of "voluntariness" remain doubtful in Canadian law. That being so, it is impossible to say that review by the courts of the circumstances in which the accused made a statement will constitute discouragement of "oppressive" police conduct in the interrogation of suspects.

15. The paucity of complaints made to us about the manner in which members of the R.C.M.P. have questioned suspects, and our examination of R.C.M.P. files, lead us to the conclusion that oppressive questioning is not widespread in the R.C.M.P. Yet there have been examples of such conduct. The *Horvath* case involved members of the R.C.M.P. Some members of the Supreme Court of Canada considered the circumstances of the interrogation found in that case to be very objectionable. The accused, a 17-year-old, was suspected of murdering his mother. He was questioned from 12:20 a.m. until 3:10 a.m. and from 12 noon until 4:16 p.m. During the first interrogation, two R.C.M.P. constables, in the words of the trial judge "hammered him with [verbal] shots from both sides" for just under three hours, and accused him again and again of lying. The trial judge found that the manner of questioning was oppressive. The trial judge found that the "atmosphere of oppression" was so great as to give the accused "a sense of being threatened". During the second period, the accused was questioned by a sergeant "trained with great skill in interrogation techniques", and the trial judge found that in all the circumstances the "complete emotional distintegration" of the accused had been brought about.

16. Another case, which we will be dealing with in detail in another Report, also involved strong judicial criticism of conduct of R.C.M.P. members in interrogating a suspect. The case raised the question not only of oppressive conduct but also the matter of the right to counsel, discussed above, and "trickery", discussed below. This was a murder case in which the accused was suspected of having killed her common-law husband. Upon being taken to police headquarters she was questioned from 7 p.m. until 2:30 a.m., at which time she was admitted to hospital, suffering from an apparently self-administered overdose of sedatives. At 9:45 a.m. she was taken from the hospital back to a police office and questioned again until some time before 12 noon. She was then placed in city police cells and later that day charged with first degree murder. The statements she made to the R.C.M.P. officers were tendered in evidence by the prosecution at her preliminary inquiry. Because of the circumstances in which they were obtained, the provincial court judge held that the statements were inadmissible and criticized the conduct of the members of the R.C.M.P. No complaint was made to us by any person involved, but because of the press publicity the case received, we inquired into it. We found that, because of the judge's comments, there had been an internal investigation in the R.C.M.P., from which the following facts emerged:

(a) The interrogation of the accused prior to her admission to the hospital was continued over a period in excess of 7 hours, part of which occurred after the R.C.M.P. members knew that the suspect had taken a sedative and was lapsing into unconsciousness.

(b) The officers continued to interrogate her after they knew that any statement which might then be obtained would be inadmissible.

(c) The officers attempted to induce a confession by reminding the suspect that if she were convicted of murder she would go to prison for life and her child would be given up to welfare and brought up an orphan.

(d) After she had had only five hours of sleep in the hospital, the interrogation continued.

(e) On more than one occasion the suspect told the officers that she wished to call her lawyer. The officers used "delaying tactics" saying that the lawyer would be called, but that a few matters had to be discussed first. (Since the suspect had talked to her lawyer before going to the police office, the officers claimed that this was not a denial of counsel but a "delaying tactic" only.)

(f) Some of the officers claimed that nothing in their training or their experience before the court led them to conclude that delay in providing counsel, when an investigative interview was in progress, was improper.

(g) Several weeks after the charge was laid, when it was intended to administer a polygraph test to the accused, a sergeant promised her lawyer that he would be allowed to see the accused immediately after the test was completed. The sergeant then broke his word and there was a further delay of several hours before the lawyer was permitted to see his client, during which the R.C.M.P. members ignored the lawyer's knocks at the door of the very room where the accused was being interviewed.

(h) Attempts to interview the accused continued even after she had been remanded, and included showing her a picture of the deceased, without seeking the permission of her lawyer to do so.

(i) After the internal investigation had been completed at the Division, a senior officer in Ottawa, reviewing the file, recorded that in his opinion more ought to have been done by the investigators on the "right to counsel" issue and that continuing the interrogation after the suspect was lapsing into unconsciousness was an error. However, he expressed the opinion that the conduct of the interrogation otherwise was "not unlike [that of] other investigators and [that] the methods used were not harsh or unusual". On the issue of the "right to counsel", this senior officer, referring to the knowledge by defence counsel that his client was being interviewed on the later occasion, put the onus on defence counsel to protect the interests of his client. The officer, in his report to the director of personnel, stated:

> It would appear that once counsel knew his client's position, it was up to him to properly advise her and ensure her rights were protected.

17. Our concern with this case is not only that experienced investigating officers believed that their conduct was proper, but that a senior R.C.M.P.

officer should come to the conclusion that it was "not unusual". There is no indication in his report on the matter that he found the conduct surprising or aberrant. This gives us cause for grave concern. If the senior officer was correct in his conclusions, then we are concerned that conduct of that type appears not to be isolated, but despite every effort we have not been able to locate other instances. On the other hand, if it is isolated and aberrant, it nevertheless does not shock the conscience of a senior officer whose responsibility lies in internal inquiries into disciplinary matters. In either case, we wish to express our concern. Our comments with respect to the conduct of the various R.C.M.P. members involved will be made when we consider this case in more detail in a subsequent Report.

Brutality

18. We are pleased to report that there is very little evidence before us to indicate that in the R.C.M.P., violence, or the threat of violence, is used to obtain statements from suspects. Once again, we have only one case before us which raises the issue. It was not a case arising from a complaint received by us. The matter came to our attention only because the trial judge happened to speak of the matter to a group of judges who by chance included the Chairman of this Commission. Even the trial judge did not at the time have any intention of placing the matter formally before our Commission. The case involved the murder of a motorist who picked up a hitchhiker, the accused. When the accused was arrested he was found to be in possession of things that afforded strong circumstantial evidence that he was the murderer. He denied any knowledge of what had happened to the deceased. Threats were made to him during two interrogations lasting a total of six hours. He was then taken to a room by an R.C.M.P. corporal and constable in plain clothes. The room was stripped of all furniture except a chair. The corporal told him to stand up and remove his spectacles, kicked him in the testicles, and hit him across the face with the back of his hand. When the accused would not answer questions, he was told by the corporal that he would be "taken for a ride". The R.C.M.P. officers then took him off in a car. They told him that they were not like other police officers, but were from a special squad, and that what he told them would not be for court purposes. The corporal struck him hard blows on the head and body that caused swellings and lumps on his head. He was told that he was being taken to a gravel pit. Afraid of what would happen there, he made a statement as to where the deceased's body could be found. This statement proved to be only partly correct, and resulted in a fruitless search for the body. Following further threats, but no further physical violence, he finally gave the correct location of the body. All these facts were placed before the judge before whom he pleaded guilty to second degree murder. The facts were placed before the court during the hearing as to sentence, by a statement of facts agreed to by counsel. The corporal submitted a detailed report of his activities, including the facts that concern us, to his superior officer, who did nothing. A week after the sentence hearing, the trial judge mentioned the matter in the presence of the Chairman of this Commission. In due course, when we enquired as to what steps had been taken internally with regard to the conduct of the officers involved, we were informed that nothing had been done

to investigate these matters. It was then, and only then, that an internal investigation was commenced in the R.C.M.P. Following the R.C.M.P. investigation, two charges of assault occasioning actual bodily harm were preferred against the corporal. No action of a criminal nature was taken against the constable, whom the Crown intended to call as a witness against the corporal. The charges against the corporal were disposed of in the provincial court where he pleaded guilty to a lesser charge of common assault. The Provincial Court judge granted the corporal an absolute discharge, largely on the ground that the corporal, in the meantime, had been medically discharged from the R.C.M.P. as a result of heart trouble, and that he had suffered sufficiently from the internal investigation and criminal prosecution. Disciplinary action was taken against the constable (who had in the meantime been promoted to corporal) for his "passive participation" in the assault on the accused, and against the officer in charge at the detachment for "failure to initiate an investigation" when he became aware of the circumstances.

19. An interesting feature of this case is that although members of the provincial Department of the Attorney General and the Provincial Court judge who presided at the preliminary inquiry were aware of the circumstances in which the statements had been obtained, no steps whatsoever were taken within the R.C.M.P., or otherwise, in regard to the conduct of the R.C.M.P. members. After our Commission took an interest in the case, the officer in charge of the C.I.B. in the R.C.M.P. Division issued a memorandum to the four officers serving directly under him expressing his "wish to be briefed as soon as possible on all serious crime incidents or unusual issues which may arise from time to time". The officer in charge has also advised that he and the Commanding Officer of the Division had had a discussion "to the effect that the C.I.B. Officer or another Officer should see major and/or sensitive files in addition to any initialling of correspondence that might be done by other C.I.B. staff members". Although we would hope that similar conduct would not occur elsewhere, its doing so remains a possibility. We therefore asked the R.C.M.P. whether any system existed in other divisions in the country to ensure that oppressive or violent conduct towards persons in custody would receive official attention. The answer given to us was that there were no similar directives in other divisions and that "one case does not a universal problem make". We are unfavourably impressed by the attitude taken by the R.C.M.P. toward this issue. Even in the Division in which measures were taken we consider that the "discussion" and the "wish" are likely to be forgotten, at least as soon as there is a change in senior personnel. The impermanence and vagueness of the "system" there afford little ground for optimism that a recurrence of such conduct would be reported to senior officers at Divisional Headquarters. The Headquarters attitude toward our request leaves us even more pessimistic about the other divisions. We hope that this kind of possible deficiency in administration would be examined by the independent review agency for police matters (the Inspector of Police Practices) which we propose in Part X, Chapter 2.

Trickery

20. In determining whether a statement made by an accused to a policeman is admissible, the Canadian courts have regarded a "trick" as having a bearing on voluntariness. For example, if the trick is a lie, it may result in the statement being held to be inadmissible if it in some way implies or at least relates to a fear of prejudice or a hope of advantage resulting in an "inducement" or "extraction" or "obtaining" of the admission.[12] The R.C.M.P. Training and Development Branch booklet on interrogation which is handed out to recruits in Regina says:

> Never lie to or deceive a suspect for, if he discovers this, he will never again co-operate. Never bluff, at least not when you may easily be discovered. If he recalls [sic] your bluff and you cannot back it up, for all intents and purposes the interrogation is over as your position is greatly weakened.

It will be noted that the limits are defined, not in terms of principle, but in terms of effectiveness.

21. Examples of a "trick" being used by field personnel are the pretences in the last two cases summarized above that what would be said would not be used for court purposes. Beyond these examples, we are unable to comment on the extent or prevalence of the use of trickery in criminal investigations.

B. SECURITY SERVICE

22. Occasionally members of the Security Service may be required to interrogate people. The suspicion will ordinarily be that the person being questioned has become the agent of a foreign intelligence agency. We do not consider that our recommendations in regard to interrogations by the security intelligence agency hinge upon the extent to which there have been such interrogations. There is only one case that we know of that has given rise to any possibility of the use of methods "not authorized or provided for by law". We shall report on it in a subsequent Report.

C. NEED AND RECOMMENDATIONS — BRIEF SUMMARY

23. It is obvious to us that both the R.C.M.P., for criminal investigation purposes and, to a lesser extent, the security intelligence agency, need to interrogate suspects in order to perform their responsibilities effectively. In Part V, Chapter 6, we shall state some concerns we have about the manner in which interrogations should be conducted by members of the security intelligence agency. Then, in Part X, Chapter 5, we shall make recommendations on the policy, reporting and review procedures and training practices of the R.C.M.P. with regard to interrogations relating to criminal investigations, and we shall also make recommendations with respect to the admissibility of illegally or improperly obtained evidence.

---

[12] *R.* v. *Materi and Cherille* [1977] 2 W.W.R. 728 at 735 (B.C.C.A.).

CHAPTER 11

ACTS BEYOND THE MANDATE

INTRODUCTION

1. In this chapter we do not examine Security Service acts or practices which were unlawful. Rather, we examine certain acts and practices of the Security Service to determine whether they were "not authorized... by law" in the sense that there was no government authority to perform them. In Part V, Chapter 3, we shall consider these same acts and practices again from the point of view of their policy implications. These two examinations will form the foundation for our recommendations for the future in regard to the matters discussed.

A. GOVERNMENT DIRECTIVES ON SURVEILLANCE ON UNIVERSITY CAMPUSES

2. Although the government did not usually devote attention to the conduct of operations by the Security Service, a specific policy was developed in the 1960s with respect to R.C.M.P. operations on university campuses. Because the policy unquestionably constituted a governmental limitation on R.C.M.P. operations on university campuses, we examine in this chapter whether the R.C.M.P. violated the policy and thus may have acted beyond its authority.

3. According to R.C.M.P. files, in June 1961 the Minister of Justice, the Honourable E. Davie Fulton, gave verbal instructions to Commissioner C.M. Harvison to suspend the R.C.M.P.'s investigations of subversive activities in universities and colleges. At the time the only activities that the R.C.M.P. deemed subversive were those of Communist organizations. Apparently a short-term freeze on operations was intended until a detailed study of the problem could be completed. Divisions were advised by letter, dated June 21, 1961, that all investigations connected with Communist penetration of universities and colleges were to be suspended, but that long established and reliable agents and contacts should be permitted to continue to report upon developments. That letter stated:

> Owing to recent unfavourable publicity arising from enquiries conducted by S. & I. personnel in connection with Communist activity amongst students, the Commissioner has directed that all investigations connected with Communist penetration of universities and colleges or similar educational institutions, is to be suspended forthwith, pending an analysis of our requirements.

2. This should not be interpreted as meaning that we have waived our interest in Communist activities within educational institutions, but rather that we must undertake a careful review of our approach to problems which could result in critical and somewhat embarrassing reflections upon the intentions of the Force. It should be made clear that no action of any kind which could result in public discussion or complaints to the Minister is to be undertaken until the review.

4. One interpretation of this instruction is that not all R.C.M.P. investigations on campus were curtailed, only those concerned with Communist activity. However, it is important to point out that at that time the R.C.M.P.'s counter-subversion programme was directed against Communist activity. Throughout the 1960s the Fulton directive was regarded within the Security Service as applying to all R.C.M.P. university operations with the exception of reports from previously established sources and security clearance investigations.

5. In 1963 the government changed, and, as a result of representations by the Canadian Association of University Teachers (C.A.U.T.), further consideration was given by the government to R.C.M.P. activities on university campuses. Meetings between the Prime Minister and the C.A.U.T. were held in July and November 1963. At the conclusion of the November meeting a public statement was issued by the Prime Minister which read as follows:

> There is at present no general R.C.M.P. surveillance of university campuses. The R.C.M.P. does, in the discharge of its security responsibilities, go to the universities as required for information on people seeking employment in the public service or where there are definite indications that individuals may be involved in espionage or subversive activities.[1]

This policy statement does not appear to have been a Cabinet decision; rather, it was an expression of present policy by the Prime Minister worked out after discussion with officials and the representatives of the C.A.U.T. and the National Federation of Canadian University Students. While it was not seen as a formal government directive by the senior management of the R.C.M.P., divisions were advised in the course of a long report on the November meeting with the C.A.U.T. that "absolute assurance was given that there was not at the present time any general security surveillance of university campuses by the R.C.M.P. nor of any university organizations as such". In 1970 and 1971 the Pearson policy statement was formally reaffirmed by Cabinet as government policy and continues as such to this day. In one respect, the Pearson statement supplemented the Fulton policy by recognizing that the R.C.M.P. might seek information on campus "where there are definite indications that individuals may be involved in espionage or subversive activities".

6. Thus, at the end of 1963 the situation was that the government had specifically directed the R.C.M.P., by means of the Pearson statement, that there was to be no general surveillance of people or organizations on campus.

---

[1] "R.C.M.P. Activities on University Campuses", *C.A.U.T. Bulletin*, Vol. 13, No. 2, October 1964.

Furthermore, the Fulton moratorium on campus investigations — specifically that no new sources on campus should be developed — had never been rescinded and the policy, insofar as the R.C.M.P. was concerned, remained in effect.

7. In the mid-1960s the Security and Intelligence Directorate of the R.C.M.P. reached the conclusion that much subversive activity had its origin in universities and colleges and it was anxious to improve its coverage of such activity. While subversive activity was still considered by the R.C.M.P. as predominantly Communist, it was no longer seen by them as exclusively so. Thus, in Quebec there was evidence that terrorist sympathizers were active in universities and other educational institutions. The Security and Intelligence Directorate therefore decided to put special emphasis on the development of sources in the university milieu, but to do this within the constraints previously imposed by government. There is no evidence that sources were developed from among students, but it is clear that a good deal of effort was devoted to the recruitment of faculty members. In an important directive to divisions, dated November 29, 1967, a senior officer in the Security and Intelligence Directorate gave instructions to develop sources on campus:

> As noted above, it is contended, with rather overwhelming supporting evidence, that university campuses are the core [sic] to these newly recognized, potential threats to national security. It is not suggested that universities, per se, are involved in conspiratorial activities directed against our democratic system, however, it is an irrefutable fact that they do exert considerable influence on sociological issues of the day and are, therefore ripe targets for communist infiltration and manipulation. You will undoubtedly agree that a person who privately harbours Communist sympathies and who gains an influential position in a select faculty on a university, can contribute immeasurably to the Communist cause. The value of such a person to the movement is obvious as is our corresponding security responsibilities. In addition to this, universities are obviously being utilized as stepping stones for infiltration of other intellectual groups and, of particular concern to us, of "key sectors" of society. It seems apparent then, that university campuses are the focal point of the entire problem.
>
> In attempting to devise ways and means of attacking this problem, many and varied methods, short of conducting on campus enquiries, have been considered and implemented. As indicated above, however, the success achieved has been negligible and leads one to question the suitability of our current techniques. In analyzing these methods it is obvious they are ineffective and completely inadequate in light of current demands. This can, for the most part, undoubtedly be attributed to the present restrictions placed, by the Government, on subversive enquiries at educational institutions. It is evident, however, that no appreciable progress can reasonably be expected in this area without the cooperation of, or liaison with, select faculty members on the universities concerned. Our experience during the past six years has clearly shown that the desired information is simply unattainable off campus and, if we are to succeed in this important undertaking, our current methods will require a degree of revision. It is felt that with tact and diplomacy we could achieve our objectives, or a good portion of them, without transgressing the assurances we have provided to the government.

It will be recalled that in 1961 the Government was assured we would refrain from conducting enquiries on subversive activities on university campuses. Instructions in that respect are contained in our memorandum of 21-6-61. . . This restriction is still in effect and, under the circumstances, we are bound to abide by this directive until such times as it is revoked. It is significant, however, that the restriction pertains exclusively to subversive enquiries with no objection being made to the conducting of legitimate security enquiries. Throughout the dispute of 1961/62 relative to our on-campus investigations the necessity of legitimate security enquiries was conceded by even our most vocal protagonists. This position was never refuted during subsequent debates and apparently, has been accepted by all concerned.

While we are morally, and indeed, honour bound to respect the assurances we made to the Government in this area, paradoxically, we are still burdened with the responsibility of keeping that same Government abreast of Communist penetration of the educational process. However, since we are under this dual obligation it is clear that the probable solution lies within the realm of security enquiries through which it is possible to establish liaison with faculty members. Such enquiries are, in fact, the only legitimate grounds on which we may establish this liaison. Since our efforts are restricted to this one avenue, we should exploit the opportunity to the fullest possible extent in keeping with our heavy responsibilities in this area. As a point of interest, the limited success we have enjoyed to date was, in large measure, accomplished through this medium.

While limited progress has been made in various areas, the success realized at one particular institution may best illustrate the use to which legitimate, on-campus enquiries may be put. Two senior investigators, well versed in [counter subversion] Branch interests, were delegated to conduct all university investigations, including the all important security screenings. Our knowledge of Communist penetration of the institution was then reviewed and, on the basis of the review, specific faculties were singled out for further study. Security investigations relating to these faculties were given particular attention with a view of eventually interviewing all professors who were not adversely recorded in our indices. All such professors listed as references on the P.H.F.s [Personal History Forms completed by applicants for employment in the public service] were interviewed without fail. Additionally, faculty heads and assistants, even though they were not specifically mentioned on the P.H.F.s, were requested to provide character references on former students seeking sensitive government employment. As part of the character study the professor was routinely invited to comment on the person's loyalty and patriotism. Needless to say, the members concerned identified themselves as members of the Force and fully explained to the professor in question the exact nature of the enquiry. Under no circumstances was the overt and legitimate nature of the enquiry deviated from.

Following each interview the investigator committed the salient points thereof to paper in a book which was maintained for the express purpose of compiling data on faculty members of the university concerned. This was, of course, in addition to the usual report on the particular [security screening] file. Each professor or staff member interviewed was allotted one page which was headed with the faculty, the professor's name and his

position. Beneath this were listed all interviews with him. These were detailed as to the date of the interview, the reason therefore. . . and most importantly, the professor's personal reaction. Special attention was devoted to his willingness, or lack of same, to cooperate with the investigator, his general attitude towards the Force and what sentiments he displayed, verbally or otherwise, to our presence on the campus.

All contacts on the campus were duly recorded and analyzed. Those who were obviously well disposed towards us and who appeared willing to cooperate, were given additional attention. Efforts were made to arrange further interviews (based, as usual, on security enquiries) during which the subject's reactions were further examined. As at the outset, subsequent interviews were restricted to the security enquiries concerned. All reactions were, however, recorded in the manner noted in the preceding paragraph. In addition to fulfilling the requirements of the enquiry, the investigators endeavoured to establish a personal rapport with the professors. This was accomplished through general conversation on far ranging topics and, in some cases, limited social contacts in the form of coffeeing or lunching together. As in the past, no effort was made to directly solicit the individual's cooperation, nor was the matter of subversion broached. Essentially, a friendship was developed with an attempt made to relegate the professional status of both the investigator and the professor, and all that that entails to, at least outwardly, a position of secondary importance.

The discussions entered into arose very naturally when our "business transactions" were completed. Besides any number of topics of no particular concern to us, many persons, because of our declared interest in "security", raised, in general terms, the subject of Communism. Under the circumstances this was considered a natural course of events. Most had very definite views and the discussions which ensued were, to say the least, of more than passing interest to the investigators. In spite of a general opinion to the contrary, it was found that many professors were not only very much aware of the threat posed by Communism but also genuinely concerned about it. Those discussions were enlightening and posed no threat to our operations since the subjects raised were covered in depth in any number of books or other publications available to the general public. Other subjects such as the international situation, the Sino-Soviet dispute, local issues (political or otherwise) were often raised in these general conversations.

One topic which, not surprisingly, was frequently raised by faculty members was the dispute raging over our "on campus" investigations. Discussions in this vein quickly determined the person's views on the matter and removed any doubts, one way or the other, the investigator might have had. In most cases, however, the issue was raised in a sympathetic manner. Occasionally, when circumstances appeared favourable, a professor would be asked outright if he had any objection to our security enquiries. This frequently led to his revealing his views on the entire question of on-campus investigations, subversive or otherwise. It is significant that, in most cases, there was no objection to any of our enquiries so long as they were conducted prudently and with discretion. A detailed account of all such discussions would be impractical at this juncture, however, a brief insight of their scope is provided by the foregoing points. No doubt the most important point is that neither the letter, nor the spirit, of the trust placed in us by the Government was broken. All contacts were legitimate, honourable and useful. Under no circumstances was the professor's formal cooperation

sought nor was the subject of subversion raised by the investigators. In short, every precaution was taken to ensure that our long range interests were not compromised. The individuals concerned were provided no opportunity to voice any legitimate complaint of unethical practices on our part.

When the foregoing plan had been pursued over an extended period of time, some rather pleasant developments took place. The most significant of these was in the number of professors, etc., who eventually offered their full cooperation on all matters of interest to us. Many, without prompting on our part, volunteered, or at least chose to discuss, the activities and political views of a number of their colleagues. It was evident that they would have spoken to us sooner but did not know anyone connected with the Security Service and would not take it upon themselves, for obvious reasons, to call our offices "blind". Once an association had been developed some individuals actually called us to pass on pieces of information of potential interest to us. This willingness to cooperate was displayed in varying degrees and in a variety of ways, however, of immense importance to us was that a workable liaison had been established. By mere social evolution our interest in subversion was also accepted and information developed without the necessity of us first providing information on persons of interest to us. This was also accomplished without the necessity of directly soliciting their cooperation.

Of further value in an operation such as that described, is the fact that, besides creating liaison with faculty members, it also determines those persons who should not be contacted. This is of positive value since it alerts us to potential problem areas which would otherwise be unknown. Such information, gained through legitimate means, could prove useful in various ways on future, unrelated enquiries. This could be of particular value relative to extremely delicate (counter espionage) Branch enquiries which very often involve this profession.

The essential point in this type of operation is that no attempt of any kind is made to solicit an individual's cooperation. What we are doing, in effect, is making ourselves known and available to the profession should any of its members have occasion, and the desire, to speak to us. Once this desire is expressed we would be grossly negligent in our duties if we refused to listen to the person. In the operation described above a number of persons did, in fact, indicate they were glad to meet us since they wished to discuss certain matters. It is assumed that, had we not made our presence known, the persons concerned would not have made any special efforts to contact us. Although persons in this profession will not usually initiate contact, it has been proven that they will confer with us if they know one of our investigators through previous legitimate dealings. Once the desired liaison has been established and continued over an extended period of time, the individual concerned really becomes an established casual source with whom we can safely deal.

It is noteworthy that in the above described operation, which has been in effect for five years, no embarrassment to the Force resulted; our assurances to the Government were not broken; standing policy within the Directorate was not contravened, yet, a workable and valuable liaison was established at the institution concerned. It should also be noted that university students were not involved in any manner in the plan. All things considered, it was a worthwhile and secure exercise which proved that, in

spite of the restrictions under which we are obliged to operate, we can discharge our responsibilities in this delicate field of endeavour.

Despite the frequent disclaimers, there is no question that the actions outlined and commented on in the directive represent a comprehensive, long range programme of source development on campus. The security screening process was being used as a means of making contact with faculty heads and assistants, even though they were not mentioned as referees on personal history forms, and persons who were obviously well disposed were re-interviewed and cultivated in the hope that a continuing relationship would be established. The method employed was subtle and indirect but its object was clear: the development of a number of faculty sources who would contribute to the counter-subversion programme.

8. On July 8, 1968, the same senior officer who had signed the letter to divisions of November 29, 1967, admitted in a letter to the Secretary of the Royal Commission on Security that the Security Service was endeavouring to develop a few sources of high reliability with respect to campus subversive activities, but these approaches were not being made on campus.

9. It also appears that in 1968 and 1969 when student violence was a serious problem, the Security Service held a number of consultations with university presidents and senior administrators at several large universities. These consultations — which were welcomed and in fact encouraged by senior university personnel — were not regarded as source development although through them a certain amount of information on subversive activities on campus was undoubtedly accumulated.

10. We have reached the conclusion on the basis of this evidence that the R.C.M.P. in the late 1960s embarked, without government approval, on a significant programme to upgrade and improve their contacts with university faculty members. This programme was undertaken in response to increasing militancy in the universities and, in some universities, the development of terrorism. Nevertheless, it appears to us that this programme was in conflict with the instructions received by the R.C.M.P. in 1961 that no new operations were to be conducted and that only established sources were to be used. It was also in conflict with government policy enunciated by Mr. Pearson in 1963 that there was no general surveillance of university campuses. In our opinion, the procedure described in the directive to divisions, dated November 29, 1967, was designed to circumvent the policy of the government and it was inaccurate to claim that such procedures complied with government policy.

11. By the end of 1970, in the aftermath of the October Crisis, the question of surveillance on university campuses again came before Cabinet. After considerable discussion the Cabinet, by a decision dated September 30, 1971, reaffirmed the 1963 Pearson directive as a statement of general policy, rescinded any other directives and ordered further

> that no informers or listening devices will be used on university campuses except where the Solicitor General has cause to believe that something specific is happening beyond the general free flow of ideas on university campuses.

After this directive it was clearly a prerequisite that the use of all sources on university campuses have the authorization of the Solicitor General. However, in a letter dated December 13, 1971, the Solicitor General advised the R.C.M.P. that this Cabinet directive would not apply

> (a) in cases of emergency, provided a report was given to the Solicitor General within 48 hours;
>
> (b) in cases where informers volunteered information to the Security Service and were not paid for the information provided.

12. It would appear that these instructions were issued by the Solicitor General after consulting the Director General of the Security Service and that the Cabinet decision of September 30, 1971, was not amended. It also does not appear that the Solicitor General knew of the number of "volunteer informers" that had been developed by the Security Service. (We note that "volunteer informers" is an ambiguous phrase as it does not distinguish between informers who volunteer and unpaid informers.) We point out that the Cabinet directive of September 30, 1971, applies in quite explicit terms to "informers" and we can see no reason to interpret it as being limited to paid sources. Furthermore, the emphasis placed by the Security Service in 1967 on the recruitment of "volunteers" suggests that this could be a significant exception. In our opinion, if the Solicitor General and the Security Service intended to adopt a narrow interpretation of the word "informers", the Cabinet should have been advised and the Cabinet directive should have been amended to make it clear that the approval of the Solicitor General was to apply to the use of paid sources only and that there should be an exception in the case of emergencies.

B. SURVEILLANCE OF LEGITIMATE POLITICAL PARTIES

13. As we shall see in Part V, Chapter 3, Prime Minister Trudeau stated in the House of Commons on May 11, 1976, that his view and that of the government, which he said had been stated in Cabinet Committee, was that

> if the party is legal, it should not be under surveillance systematically by the Royal Canadian Mounted Police or any other police.[2]

Mr. R.G. Robertson, who was Secretary to the Cabinet in the 1960s and Chairman of the Security Panel, considers that this has represented the policy of the government since 1964. He testified that at that time the concern was about the Rassemblement pour l'Indépendance Nationale (R.I.N.), a predecessor of the P.Q. He said that

> the R.I.N., as a legitimate political party, was not supposed to be subject to the kind of surveillance that there would be of a terrorist organization or a subversive organization. So that the R.C.M.P. had to operate under that disability, that they could not have surveillance of the R.I.N. as such.
>
> (Vol. C107, p. 14068.)

---

[2] House of Commons, *Debates*, May 11, 1976, p. 13389.

Mr. Robertson was referring to a decision of the Security Panel on September 23, 1964, chaired by himself, to recommend to the Cabinet that the R.C.M.P. be authorized, in security screening matters, to include in their report to departments

> the fact of membership in open organizations such as the R.I.N. together with the detailed information concerning length of attendance, degree of involvement and other pertinent information as was available, in order that the department, on whom final decision for the clearance rested, could consider the necessity of further investigation, as they would do in cases of information concerning membership in the Communist Party, front organizations or character weaknesses.
>
> (Ex. MC-182, Tab 2.)

He says that the words "other pertinent information as was available" contemplated that the R.C.M.P. "might get that information from heaven knows what sources, and if they had it they should produce it. But the R.I.N. was not subject to surveillance" (Vol. C107, pp. 14066-8).

14. On May 6, 1976, Mr. Allmand had told the House of Commons that the Cabinet's decision had

> ... confirmed that the R.C.M.P. should not survey legitimate political parties per se, but of course individuals in all political parties should be subject to surveillance if they are suspect with regard to criminal activities, subversion, violence or anything like that.[3]

This explanation corresponds with what Mr. Dare had written in a letter to some senior officers on June 9, 1975, with regard to "criteria used to investigate the Parti Québecois and its members". He said that

> The Prime Minister stated that the Security Service of the R.C.M.P. does not have a mandate to conduct these enquiries unless they fall within Items A to F of the Cabinet Directive of March 27, 1975.

15. If Prime Minister Trudeau's statement of May 11, 1976, were taken alone, one might infer that systematic surveillance by the Security Service of any "legal" party was not permitted. If that were so, an issue would arise as to whether the R.C.M.P. has conducted systematic surveillance of certain parties that are "legal", in the sense that they are not prohibited from organizing as political parties and that they nominate candidates in federal, provincial and municipal elections. The issue arises in respect to such parties as the Communist Party of Canada, the Communist Party of Canada (Marxist-Leninist), the New Democratic Party's Waffle Movement and the Parti Québecois. If the proper conclusion is that there has been systematic surveillance of such parties, the question then is whether it can be said that such surveillance was beyond the authority of the Security Service — i.e. whether, in the language of our terms of reference, it was "not authorized... by law".

[3] *Ibid.*, May 6, 1976, p. 13224.

16. The Royal Commission on Espionage, established as a result of the defection by Mr. Igor Gouzenko, reported in 1946 that the evidence "overwhelmingly" established

> that the Communist movement was the principal base within which the espionage network was recruited; and that it not only supplied personnel with adequately "developed" motivation, but provided the organizational framework wherein recruiting could be and was carried out safely and efficiently.
>
> In every instance but one, Zabotin's Canadian espionage agents were shown to be members of or sympathisers with the Communist Party...
>
> The evidence shows that the espionage recruiting agents made use in their work of reports, including psychological reports, on Canadian Communists which had been prepared as part of the routine of the secret "cell" organization of that Party...
>
> ...A preliminary feeling out of the selected recruit, before the latter realized the sinister purposes for which he was being considered, could also be made within the framework of normal Communist Party activities and organization, and there is also evidence that this was part of the technique of recruiting.[4]

The Commission then gave a detailed example of three scientists who were recruited from among the secret members of the Communist Party. The Commission concluded its exposition of this example by saying:

> Thus within a short time what had been merely a political discussion group, made up of Canadian scientists as members of a Canadian political party, was transformed on instructions from Moscow into an active espionage organization working against Canada on behalf of a foreign power...
>
> The evidence also discloses that secret members of the Communist Party played an important part in placing other secret Communists in various positions in the public service which could be strategic not only for espionage but for propaganda or other purposes.[5]

17. The Report of the Royal Commission on Security in 1969 observed that

> it seems clear that the main current security threats to Canada are posed by international communism and the communist powers, and by some elements of the Quebec separatist movement. The most important communist activities in Canada are largely directed from abroad, although domestic adherents of and sympathizers with communism pose considerable problems in themselves...[6]
>
> The communist powers conduct espionage and subversive operations ... through members of the communist parties in Canada, both overt and underground...[7]

---

[4] *Report of Royal Commission on Espionage*, 1946, pp. 44-5.
[5] *Ibid.*, at pp. 47 and 49.
[6] *Report of Royal Commission on Security*, 1969, para. 14.
[7] *Ibid.*, para. 16.

> As far as the trade union movement is concerned, there is a long history of attempts by the Communist Party to assume control at local levels and to take all possible measures to influence national policies; these attempts are usually, but not always, frustrated.[8]

The Commission made no observations as to whether the Communist Party of Canada was otherwise a threat to national security, or if it was, in what respects it was. We have no reason to disagree with any of the passages just quoted.

18. As a political party, the Communist Party of Canada has received only minimal electoral support. Since the conviction of Fred Rose, M.P. in 1947, there has never been a Member of Parliament elected under the auspices of the Communist Party of Canada. If the Party received more electoral support than it does, the grounds upon which its activities would be watched would be more obvious than they have been. The grounds on which surveillance has been justified have been the features noted by the Royal Commission in 1946: that the Party is a breeding ground for espionage, and that its secret members attempt to penetrate the government.

19. Both those grounds have been recognized by the government of Canada over the years as bases for the following intelligence activity by the R.C.M.P.:

(a) In the 1950s and 1960s the Advisory Committee on Internments, established and continued by successive Ministers of Justice, received "evidence briefs" from the R.C.M.P. on organizations which the R.C.M.P. proposed should be classified as "recognized Communist organizations". If so classed by the Committee, then, in an emergency, the organization could be declared an illegal organization under regulations adopted pursuant to the War Measures Act. The Advisory Committee was also to place names on a list of members of those organizations who were "prominent functionaries", and who would be interned in the event of a national emergency. In order that this system could operate, it was obviously necessary that the R.C.M.P. have accurate and positive proof of membership in the Party or other organizations. The Committee itself fell into decline in the late 1960s, but the collection and analysis of the same kind of intelligence has continued within the R.C.M.P. to the present time.

(b) Cabinet Directive 35, which has been the foundation for security screening in the Public Service since December 18, 1963, provides that the Government of Canada cannot place confidence in persons who are required to have access to classified information in the performance of their duties, if their "loyalty to Canada and our system of government is diluted by loyalty to any Communist, Fascist, or other legal or illegal political organization whose purposes are inimical to the processes of parliamentary democracy". It states that the following persons

> must not, when known, be permitted to enter the public service, and must not if discovered within the public service be permitted to have access to classified information:

[8] *Ibid.*, para. 18.

(i) a person who is a member of a communist or fascist party or an organization affiliated with a communist or fascist party and having a similar nature and purpose;

(ii) a person who by his words or his actions shows himself to support a communist or fascist party or an organization affiliated with a communist or fascist party and having a similar nature and purpose;

(iii) a person who, having reasonable grounds to understand its true nature and purpose, is a member of or supports by his words or his actions an organization which has as its real objective the furtherance of communist or fascist aims and policies (commonly known as a front group);

(iv) a person who is a secret agent of or an informer for a foreign power, or who deliberately assists any such agent or informer;

All departments of the government have expected the R.C.M.P. to give them information concerning applicants for positions in the public service so that the departments may decide whether the applicants fall within any of these categories. It is obviously impossible for the R.C.M.P. to provide this information without employing informers and other intrusive methods.

(c) When the Cabinet issued a Directive on March 27, 1975, defining the mandate of the Security Service (apart from its security screening functions, as was later made clear), the R.C.M.P. made it known that it considered that the authority that was requested would, if granted, be taken as permission to "monitor" the activities of (*inter alia*) Communists, Trotskyists and Maoists.

20. The inevitable conclusion is that there has been systematic surveillance of the Communist Party of Canada, and that there has been ample governmental authority for the systematic surveillance of the Communist Party of Canada and its members. It would be playing on words to assert that it has not been the Party but only certain of its members who have been under surveillance. No such distinction can reasonably be drawn when the surveillance is of the Party's leaders and officers, and is aimed at determining their every word and action. This very surveillance has been expected by government. Therefore it would not really be accurate to say that the Security Service has lacked authority from the government to conduct systematic surveillance of the Communist Party of Canada. Moreover, even if, as we think is the case in law, the Prime Minister's public statement or a Cabinet Directive cannot be taken as having effect in *law* as authority for the R.C.M.P. doing or not doing a thing, section 5 of the R.C.M.P. Act does give the Solicitor General power of direction. So what Mr. Allmand directed would have the authority of statute behind it, and we think that his public statement in the House of Commons on May 6, 1976, would have the status of a directive. That statement was that the R.C.M.P. "should not survey political parties per se". But that statement must be qualified by the fact that Mr. Allmand, like other Solicitors General, did authorize surveillance of the Communist Party of Canada. His doing so would be a "direction" under section 5. Consequently, the R.C.M.P. has had lawful authority to conduct systematic surveillance of the Communist Party; conse-

quently its systematic surveillance of this legal party has not been an investigative activity "not authorized. . . by law".

The Communist Party of Canada (Marxist-Leninist)

21. The activities of this Party have been under intensive investigation in the 1970s. Its leader has been the object of both close surveillance and certain of the disruptive tactics which were carried out under the "Operation Checkmate" umbrella. In 1972, when it ran a number of candidates in the federal election as "independents", the Security Service drew the true nature of these candidates to the attention of the press. As a result at least one newspaper published an article as to their true identity not long before election day. The Party's electoral support in the four federal elections of the past decade has been minimal.

22. There was governmental authority for the Security Service's interest in this Party. The basis of this has been the Security Service's view that the Party is "a self-styled revolutionary party whose activities are aimed at abolishing our parliamentary system of government by force or violence and replacing it with a worker dictatorship".[9] In addition, we have seen that when the Cabinet Directive of March 27, 1975, was issued, the R.C.M.P. made it known that the authority sought, if granted, would be taken as permission to monitor the activities of Maoists. The latter category was at that time represented by the Communist Party of Canada (Marxist-Leninist). In regard to this Party the same conclusion applies as that stated in regard to the Communist Party of Canada.

The New Democratic Party

23. The New Democratic Party has been in existence since 1961. It describes itself as a social democratic party. It succeeded the C.C.F. (Co-operative Commonwealth Federation), which had been founded as a socialist party in 1932. First the C.C.F. and then the N.D.P. elected Members to Parliament in every federal election since 1935. In the past decade the Party has received between 15.4 and 19.7 per cent of the popular vote in federal elections, and elected from 16 to 32 members. It has formed the provincial government in Saskatchewan most of the years since 1944, in British Columbia from 1972 to 1975, and in Manitoba from 1969 to 1977. It has formed the Official Opposition, and for many years it has been represented by significant numbers of members, in the Ontario legislature.

24. As we shall see in Part V, Chapter 3, in the early 1970s the R.C.M.P. Security Service conducted an investigation of the Waffle Movement, which was a faction within the N.D.P. The Security Service believed that Trotskyists and Communists were joining the Waffle in order to influence its members and attempt, through it, to take control of the N.D.P. nationally and provincially. It

[9] The words quoted are from an application for a warrant under section 16 of the Official Secrets Act.

sought and obtained intelligence on the activities of those individuals within the Waffle Movement and of the Waffle Movement within the N.D.P. It even volunteered information to one leader of a provincial New Democratic Party on the basis that he should be aware of subversives within his Party.

25. Some of the language used by members of the Security Service in their instructions, reports and their analysis of the objectives of their work in this area shows that they regarded their task as the surveillance of "left-wing" members of the N.D.P. For example, one of the stated types of information which was sought was simply "The Waffle Movement". General instructions were given by Headquarters to all field personnel as follows: "We are interested in determining national aims, strategies and planned tactics of the Waffle leadership, especially when insights we develop go beyond their open, public announcements". On the other hand, there is some evidence that the rationale for the investigations was understood to be for the more limited purposes we have stated. It may therefore be that there was an imprecise understanding that varied from person to person, as to what the rationale was. Whether or not surveillance of one faction of the New Democratic Party constituted systematic surveillance of a political party is very much a matter of definition. On balance, we believe that the investigation was understood within the R.C.M.P. not to be an investigation of the N.D.P. as a whole but rather of certain persons in one faction of that party. It follows from this conclusion that it would be unfair to characterize what occurred in practice as surveillance of a political party. Therefore, in our view, the investigation did not lack lawful authority. If we are wrong in this, we can nevertheless say without hesitation that we have found no evidence of any governmental or lawful authority to conduct systematic surveillance of the New Democratic Party. In Part V, Chapter 3, we shall discuss this matter from the point of view not of lawful authority but of its policy implications. Our concern there will be to identify some undesirable features of this episode and to make suggestions how these undesirable features can be avoided in the future.

The Parti Québecois

26. The Parti Québecois was formed in 1968 as a provincial party in Quebec, an official principal goal of which was described by the Party as sovereignty association. That goal was regarded by some of its members and some of its opponents as separatism. The concept includes the establishment of a nation separate from Canada politically. It ran candidates in the provincial elections of 1970 and 1973, in which it obtained 23 and 30 per cent of the electoral vote respectively, and from 1972 to 1976 it formed the Official Opposition. At the election of November 15, 1976, it obtained 41.4 per cent of the popular vote and formed the government.

27. In Part V, Chapter 3 we shall point out that in the late 1960s the federal government expected the R.C.M.P. to obtain information about membership in, and the finances of, separatist organizations. From this it was not unreasonable that the R.C.M.P. would infer that it had the authority to investigate the Parti Québecois. Additional reasons for the R.C.M.P.'s interest in the P.Q. from 1968 onward are discussed in that chapter. So are the difficulties

encountered by the Security Service from 1975 onward in determining just what its authority was in regard to the P.Q. and its members, under the Cabinet Directive of March 27, 1975.

28. An example of the R.C.M.P.'s interest in the P.Q. *per se* is found in instructions sent by Headquarters to "C" Division in Montreal in August 1970, directing that intelligence be obtained concerning the Parti Québecois, if possible at the highest level. The reason given was that the P.Q. was a group dedicated to the dissolution of Canada:

> It is our responsibility to inform the government of any, and all, groups or organizations that are dedicated to the dissolution of Canada. The Parti Québecois is clearly and publicly committed to the dissolution of Canada as it presently exists. It will, therefore, be our responsibility to monitor the various political influences which will infiltrate the Parti Québecois and also any policy decisions as it may involve plans for seditious activity or foreign involvement. We will not require detailed information en masse, as is the case with recognized subversive organizations, however, we should develop the capability of identifying and assessing the influential functionaries. . .

It is of further interest to note that the Headquarters instructions no longer regarded the justification for "this type of investigation" as being that the only interest was in possible terrorist activities or subversive infiltration.

29. As of 1972 the Security Service's position was that, as Mr. Starnes said in a letter to Mr. Bourne on September 25, 1972,

> Our Service is not engaged in the investigation of the Parti Québecois per se. The information that we have gathered on the Parti Québecois is incidental and comes to us through our investigation of the Quebec Revolutionary Movement as well as through the media and other overt sources.
>
> (Ex. MC-158.)

Mr. Starnes appears to have believed the statement in the first sentence of the passage quoted to be true. Thus, in a May 21, 1971, memorandum for file, not designed to be read outside the Security Service, he recorded that on that day he and Commissioner Higgitt had had a discussion with Mr. Goyer in which Mr. Starnes reasoned that the government could be seriously criticized if the Security Service assisted the efforts of the Liberal Party "to oppose and to defeat the aims of a political party such as the Parti Québecois". The criticism would be "for attempting to use the facilities of the Security Service to carry out political action, of one kind or another, against a duly constituted political party in Canada". Mr. Starnes added:

> I said that it was true that the Security Service had for some years taken an active interest in the Communist Party of Canada. However, in practical political terms, this was very different from directly supporting political action against the Parti Québecois.
>
> (Ex. MC-15, Tab G.)

30. As we have seen above, Prime Minister Trudeau and Mr. Allmand made it clear in 1976, in the context of questions about the surveillance of the P.Q.,

that individuals in a legal political party should not be subject to systematic surveillance unless their activities fall within the Cabinet Directive. Since then, the category upon which the Security Service has relied in instructing paid sources within the Parti Québecois has been "foreign intelligence activities directed toward gathering intelligence information relating to Canada". This rubric has been thought to justify the collection of intelligence concerning communications by foreign governments with the P.Q. government of Quebec. Nevertheless, other information has been obtained and not rejected as being irrelevant to the proper concerns of the Security Service, on matters of certain importance to the Parti Québecois. Some of the information gathered has been passed on by the Security Service to senior officials of the Public Service of Canada without receiving any criticism in return for having collected it, even though it is unrelated to any of the categories in the Cabinet Directive.

31. Thus, even since 1976, whether it has sought the information or has been the "passive" recipient of it, the Security Service has acted beyond its mandate by receiving such information and retaining and using it. The Security Service has, by receiving such information from its human sources, paid or otherwise, received information unrelated to the categories of activities itemized in the Cabinet Directive. Moreover, the kinds of information cannot be described as other than surveillance of a legal political party *per se*. The passage of time and the number of people involved make it extremely difficult to determine whether information of this sort, when received by the Public Service, has been transmitted to Ministers as a matter of course. If it has been, then, to the extent that Ministers have received the information without criticizing the Security Service, we do not feel that we should be more critical of the Security Service for having acted outside its mandate than of the Ministers who fixed the mandate in 1975.

32. We add that here we are discussing solely the issue of acting outside the authority of the mandate, and not any question of whether some illegality was committed by the manner in which the information was obtained.

33. In our review of this matter, we came to the view that there was an apparent disregard in practice by the Security Service of the government's attempt, in regard to the Parti Québecois, to limit Security Service investigations to such activities of its members as fell within the 1975 Cabinet Directive, which is illustrated by the following example from files. Before the provincial election in 1976 a memorandum to the Deputy Director General (Operations), read by Mr. Dare reported that the Service should not inquire into "legitimate activities" within the Parti Québecois but rather that their "main interest" was one of the six activities set out in the 1975 mandate. However, the genuineness of this purported self-limitation to matters within the "mandate" is put in question by the fact that a year earlier, an R.C.M.P. memorandum stated a specific area of interest was to be pursued. The area of interest was not one set out in the 1975 mandate. Again, after the electoral victory of the P.Q., and eighteen months after Mr. Dare had made known the limitations on the investigation of the P.Q., and R.C.M.P. officer wrote a memorandum in which he observed that a particular investigative technique would enable the Security

wrote a memorandum in which he observed that a particular investigative technique would enable the Security Service better to fulfill its mandate. He suggested that the technique be used to obtain information on "generalities which may be very important to the central government but have little to do" with any of the six activities set out in the 1975 mandate. He clearly expected the technique would be used to obtain information "concerning" members of the P.Q. Government. This recommendation was concurred with by a more senior officer. The conscious determination to develop the investigative technique beyond the authority given by the "mandate" is reflected still further by a memorandum to file, written a few days later by the same member. Again discussing the same investigative technique, he contemplated that information obtained would concern the P.Q. and "should help us to prepare realistic briefs for Government". A senior operational officer read that memorandum without expressing disapproval.

34. An R.C.M.P. Headquarters file disclosed another aide-mémoire written in 1978 by an officer on the same topic which indicated that the investigative technique would, on occasion, result in additional information being obtained which fell outside the Security Service mandate. According to the aide-mémoire, such information would not be sought, but if it came to the attention of an investigator when he was dealing with mandate matters, he was to report it in any event. Such information would "generally" concern "policy and direction of the Government of Quebec" and was described as being "of obvious value to the federal government in terms of national unity". The aide-mémoire records that the matter had been discussed with a senior operational officer and that "as for passing information to government, a decision will be made in each case as to whether material will be passed because of its possible bearing on national security". As we have said, there is therefore evidence that since the 1975 mandate and public announcements about surveillance of legitimate political parties, the Security Service has actively sought information about the P.Q., unrelated to the Security Service mandate.

The Liberal Party of Quebec

35. We have some evidence that from 1970 to 1976, while the Liberal Party of Quebec formed the government of that province, the Security Service collected intelligence about certain aspects of the activities of that government and at least one paid human source had access to sensitive information about that government's policies and its ministers. That source's objectives were defined in 1971 as follows:

1. The development of information on certain diplomatic personnel in Quebec.
2. To identify the disposition, propensity and ability to exercise influence, of independentists employed in the government of Quebec and other key sectors, who use their position to promote the separation of Quebec from Canada.
3. To determine the degree of influence that revolutionary or independentist influenced or controlled pressure groups (social, fraternal and political) have on the Quebec government.
4. To determine the influence independentists and revolutionary sympathizers may have over the policies of [a certain department of the

provincial government] particularly in its relations with other French-speaking countries.

36. In 1973, the source's handler commented on a detailed report that the source had given. We have not seen the report, but the handler described it as relating to infighting between individuals in ministries in the government of Prime Minister Bourassa. The handler commented that the report made evident that there were not very many individuals who are "died [sic] in wool separatists at the very upper levels of the various Ministries, however, at the lower level ... there are a number of individuals who harbour separatist sympathies". The handler also stated that the source reported that the Quebec Liberal Party had infiltrated the Parti Québecois at a very high level. The handler concluded that the report

> enables us to keep a close watch on individuals within the Bourassa Government and this I feel is extremely important as it enables us as a Security Service to be more fully aware of upcoming policies and activities within the Provincial Government of Quebec. I feel that as a Security Service it is one of our duties to be aware of what is happening in Quebec even if the government formed is of a federalist nature.

37. At almost the same time as the making of the report by the handler, officers at a senior level authorized the handler to instruct and to stress to the source that his objectives were not to report on the government of Quebec *per se*, but that he was to report on revolutionary individuals in the government of Quebec and on individuals responsive to foreign powers, and in addition he might report any information which we might pick up from governmental policy or governmental activities of a nature which he considered was "detrimental concerning the continuation of Quebec within Confederation".

38. For our purposes in the present context to draw a distinction between the Liberal Party of Quebec and the government which it formed would be irrelevant. It is clear that the source reported and was expected to report not only on public servants but on elected members of that government, far beyond any interest in foreign interference in Canadian affairs or foreign intelligence activities. We know of no mandate which the Security Service had before March 1975, to collect intelligence on such matters, and it would be clearly unacceptable under the 1975 Mandate.

The Liberal Party of Canada

39. The Liberal Party of Canada, when in power as the Government of Canada, may be said to have been of interest to the Security Service even though the information received cannot be said to relate to the mandate of the Security Service. An unpaid source reported to the Security Service from his vantage point which, as his handler reported in 1975, enabled him to "receive rather confidential information ... on Liberal strategy, and elected members."

40. According to the file, the source has provided information about the marital problems of two Ministers, suspicions entertained by some Ministers that the R.C.M.P. was directing a plot against the government, and proceedings in the Liberal caucus. None of this information was relevant to the security of Canada, as defined by the Cabinet Directive. The receipt, recording and reporting of this information was completely unauthorized and without justification.

PART IV

REASONS ADVANCED IN JUSTIFICATION OF ACTIONS "NOT AUTHORIZED OR PROVIDED FOR BY LAW"

INTRODUCTION

CHAPTER 1: Legal Defences

CHAPTER 2: Extenuating Circumstances

INTRODUCTION

1. In Part III we analyzed a number of investigative practices that may be unlawful. The picture is incomplete unless we also discuss defences that might be raised to exonerate those carrying out such practices. Our insistence throughout this Report that the national police force and the security intelligence agency should obey the law would be mere rhetoric if there were accepted defences that would make their conduct in carrying out those practices lawful. In the first chapter of this part of our Report we shall examine whether any of these arguments do in law constitute defences if members of the R.C.M.P. were to be charged with offences under the Criminal Code or other federal or provincial statutes, or have civil actions brought against them. In the second chapter we shall examine whether, if they are not defences to a charge or action, they may nevertheless be relied upon by members of the R.C.M.P. as factors justifying compassion or mercy, before prosecution or after conviction.

2. As will be seen these issues cannot be examined as if the courts have ruled decisively on their application to policemen. Even if there were more judicial authorities directly on point, police forces should not expect certainty and predictability in the application of principles to particular factual situations.

3. There is a further introductory point to be made. Even if one or other of these defences were to be available, if a particular investigative technique is adopted as a matter of practice or particular conduct is planned in a specific situation, it does not follow that the R.C.M.P. should adopt the practice or engage in the conduct. The availability in law of one of these defences ought not necessarily to be regarded as giving the green light from the policy point of view.

CHAPTER 1

LEGAL DEFENCES

A. SUPERIOR ORDERS — MISTAKE OF FACT AND MISTAKE OF LAW — RELIANCE ON APPARENT AUTHORITY — NECESSITY AND DURESS

(a) *Superior orders*

4. Can a policeman rely on the plea of obedience to the orders of his superior as a defence to a criminal or other charge? Judicial precedents are scarce. The problem has usually been considered in a military context and as a matter of international law.[1] However, it would appear that the answer is "no": obedience to superior orders is not generally regarded as a valid defence in criminal or civil law. There have been some judicial statements concerning the position in domestic law. For example, in an English case which was actually concerned with duress, Lord Salmon stated that the defence of superior orders

> ... has always been universally rejected. Their Lordships would be sorry indeed to see it accepted by the common law of England.[2]

In an earlier case, the then Lord Chief Justice of England said:

> I hope the day is far distant when it will become a common practice in this country for police officers to be told to commit an offence themselves for the purpose of getting evidence against someone; if they do commit offences they ought also to be convicted and punished, for the order of their superior would afford no defence.[3]

A leading authority on criminal law has written that

> ... it is an established principle of constitutional law that official position and superior orders (whether of the Crown or of a private master) are not in themselves a justification for committing an act that would otherwise be a legal wrong.[4]

---

[1] See M.L. Friedland, *National Security: The Legal Dimensions*, Ottawa, Department of Supply and Services, 1979, at p. 104; L.C. Green, *Superior Orders in National and International Law*, Leyden, A.W. Sijthoff, 1976. See also Geoffrey Creighton, "Superior Orders and Command Responsibility in Canadian Criminal Law" (1980) 38 *U. of Toronto Law Rev.* 1.

[2] *Abbott* v. *The Queen* [1976] 3 All E.R. 140 at 146 (P.C.).

[3] *Brannan* v. *Peek* [1947] 2 All E.R. 572 at 574 (K.B.D.).

[4] Glanville Williams, *Criminal Law: The General Part* (2nd ed.), London, Stevens, 1961, at p. 296.

5. Alongside these dicta, which were expressed in the context of English criminal law, reference must be made to views expressed by several Justices of the Supreme Court of Canada. Thus, in *Chaput* v. *Romain*[5] and again in *Chartier* v. *A.G. Quebec*[6] the view was advanced, with specific reference to the legal position of police officers, that "a subordinate is not necessarily exempt from liability because the wrongful act was committed in order to comply with a superior's order".[7] In *Chaput* v. *Romain* the Supreme Court held police officers who obeyed their superior's order liable civilly, and Mr. Justice Taschereau, whose decision was concurred in by three other members of the Court, spoke of the law as to superior orders as follows:

> [Translation] Furthermore, no reliance can be placed on the fact that the respondents may have acted in obedience to a superior's orders. Obedience to a superior's orders is not always an excuse. The subordinate must not act rashly, and when he is made reasonably aware that the facts which led to the order he received were without foundation *he must back down.*[8]

This statement was cited with approval by four Justices of the Supreme Court of Canada in the *Chartier* case. It evokes distinct echoes of the principle that once prevailed in the area of military law, to the effect that the defence of superior orders could be successfully relied upon only if the order was not manifestly unlawful.

6. Modern international and military law has tended to deny the defence even when the order was not manifestly unlawful. Whatever the scope of the defence in military law, the analogy between the soldier and the policeman is not generally helpful. It is understandable that at least a limited defence of superior orders might be argued for in the armed forces where, at least in battle, there is a need for military discipline requiring prompt obedience.[9] There may be an analogy in police work when there is sudden violence or some other emergency, but in the kinds of investigative practices which we have examined, there is usually no such situation. These practices and acts involve careful preparation and ample time for reflection and refusal to participate. It cannot be said in these cases that a failure to obey promptly will imperil the safety of fellow policemen.

7. Our view is that in the present state of Canadian law it is doubtful that a member of the R.C.M.P. would, at least in the absence of sudden violence or some other emergency, be able to raise successfully a defence of superior orders to a charge under the Criminal Code or any other federal or provincial statute.

8. However, it must be noted that a defence of a superior's order may be relevant to the limited extent to which mistake of law gives rise to a defence. Moreover, there may be situations in which the superior's order will cause a policeman to labour under a mistake of fact, causing him to lack the intent

---

[5] [1955] S.C.R. 834

[6] (1979) 9 C.R. (3d) 97.

[7] Per Mr. Justice Pratte in *Chartier* v. *A.G. Quebec*, *ibid.*, at p. 177.

[8] [1955] S.C.R. 834 at 842, quoted in English in *Chartier* v. *A.G. Quebec*, (1979) 9 C.R. (3d) 97 at 155.

[9] See Glanville Williams, *Criminal Law: The General Part* (2nd ed., 1961), p. 298.

necessary for crime (*mens rea*). We turn now to a discussion of mistake of law and mistake of fact.

(b) *Mistake of fact and mistake of law*

(i) *Mistake of fact*

9. General propositions as to the availability of mistake as a defence to a criminal charge are difficult to express in categorical terms.[10] Indeed, it is doubtful if any propositions on the subject of mistake have a universal application. So much depends on the definition of particular offences and whether proof of *mens rea*, a guilty mind, is an essential element that must be established by the prosecution. To ignore the various qualifications that govern the availability, in criminal cases, of a plea of mistaken belief is to run the serious risk of misstating the law, or justifying questionable conduct by invoking legal principles that have a very limited application.

10. Several alternative circumstances need to be considered, the nature of which will dictate the scope of mistake as a legal defence. First, it is open to the legislative body, when it defines an offence, to state the criteria by which a mistaken belief must be judged. Where it does so, the mistake must be judged by an objective standard, in other words, according to whether a reasonable person would have been mistaken in the light of the prevailing circumstances. Anything less will not constitute a defence however genuinely mistaken the accused might have been. Examples of this category are to be found in the crime of extortion "without reasonable justification or excuse" (Criminal Code, section 305), or in pleading self defence which requires that the accused "believes, on reasonable and probable grounds that he cannot otherwise preserve himself from death or grievous bodily harm" (Criminal Code, section 34(2)). Other examples will be found in our recommendations with respect to the unauthorized disclosure of government information, in our First Report.[11]

11. The second situation relates to those offences which abound outside the Criminal Code, in federal and provincial statutes, and which are described as offences of strict or absolute liability. This means that there is no requirement of proving *mens rea*. Ordinarily, that would end the matter so far as invoking a defence of mistake is concerned. Recently, however, the Supreme Court of Canada in *R.* v. *Sault Ste. Marie*[12] has declared it to be the Canadian law that, unless Parliament or the legislature of a province has made its intention clear when defining the offence in question that liability is absolute, with no question of fault being involved, it is open to the accused to avoid liability by proving that he took all reasonable care in the circumstances. This defence, the Supreme Court has ruled, will be available "if the accused reasonably believed

---

[10] For a more detailed discussion, see J.Ll.J. Edwards, *Mens Rea in Statutory Offences*, London, Macmillan, 1955, Chapter XI.

[11] Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *First Report, Security and Information*, Ottawa, Department of Supply and Services, 1979, paras. 58 and 59.

[12] (1978) 40 C.C.C. (2d) 353.

in a mistaken set of facts which, if true, would render the act or omission innocent or if he took all reasonable steps to avoid the particular event".

12. In thus recognizing a potentially wide field of application for the defence of mistake of fact, it needs to be emphasized that the defence, in the context referred to above, has nothing to do with proof or disproof of *mens rea*. The principle expressed in the *Sault Ste. Marie* case comes into play only where the particular offence is interpreted in a manner that excludes the requirement of proving a guilty mind. Normally, establishing the requisite *mens rea* in a criminal offence is part of the prosecution's burden of proof. In the special circumstances outlined by the Supreme Court of Canada in the *Sault Ste. Marie* decision, however, it is open to the accused to exempt himself from criminal liability by showing that he was mistaken as to fact and that the mistake was one that a reasonable man would have made in similar circumstances.

13. The third situation — the one which has generated the most controversy surrounding the proper test to be applied — concerns those crimes that specifically require proof of *mens rea*. Proving a guilty mind involves proving that the accused had knowledge of the various factual elements that constitute the offence in question. This may involve proof of intention or recklessness or knowledge to the requisite degree. If it can be shown that the accused was mistaken as to one or more of the essential elements, it follows that the prosecution has failed to establish that the accused had the necessary *mens rea* and, therefore, the accused cannot be held criminally responsible. This defence is open to an objective and a subjective interpretation. Those who favour the objective interpretation argue that, not only must the mistake occur and be shown to have genuinely occurred, but it must also be shown to have been a reasonable mistake. By thus setting the standard of exemption at the level of ordinary, reasonable people, the likelihood of fanciful defences of mistake being successfullly raised in a criminal case is severely reduced. Proof of the necessary *mens rea*, however, is concerned with the actual state of mind of the accused, not with the mental state of some hypothetical person. How can these two positions be reconciled?

14. The courts have recently accepted the subjective interpretation but it will be seen that they recognize that the reasonableness of belief may be relevant as to whether the accused believed in the existence of the fact in question. After two judgments[13] delivered recently, one in the Supreme Court of Canada and the other in the English House of Lords, it can now be stated that in cases involving a defence of mistaken belief the essential question is whether the belief entertained by the accused is an honest one and that the existence or non-existence of reasonable grounds for such belief is merely relevant evidence to be weighed by the tribunal of fact in determining such essential question. This principle does not state that an accused person is entitled to be acquitted however ridiculous his story might be. Neither does it imply that the reason-

[13] *Pappajohn* v. *R.* (1980) 14 C.R. (3d) 243 (Sup. Ct. Can.); *D.P.P.* v. *Morgan* [1976] A.C. 182 (House of Lords).

ableness or unreasonableness of his mistaken belief is irrelevant. The present law was expressed by Mr. Justice Dickson when he stated:

> . . . the accused's statement that he was mistaken is not likely to be believed unless the mistake is, to the jury, reasonable. The jury will be concerned to consider the reasonableness of any grounds found, or asserted to be available, to support the defence of mistake. Although 'reasonable grounds' is not a precondition to the availability of a plea of honest belief. . . those grounds determine the weight to be given the evidence. The reasonableness or otherwise of the accused's belief is only evidence for or against the view that the belief was actually held and the intent was therefore lacking.[14]

Put more shortly, the reasonableness or unreasonableness of the mistake is a question that goes to the credibility of the defence put forward by the accused. That is a matter of evidence in each individual case. It is no longer the governing criterion in cases of mistake, except in the two situations previously described in this chapter.

(ii) *Mistake of law*

15. So far we have been considering the nature and scope of a defence based on a mistake of fact. Many of the situations that we have examined involving the activities of the R.C.M.P., suggest, however, that the officers acted in the belief that they were lawfully entitled to act as they did. What is their position under the criminal law if the mistake in question is not as to the facts but as to the law? If the mistake is concerned with the existence of a legal prohibition that forbids the doing of the act in question, in other words if it is a mistake as to whether the particular conduct that is complained about is or is not a crime, the answer generally is that such a plea is no defence to a criminal charge. For reasons of public policy, ignorance of the law is not an excuse for committing an offence. Derived from English common law, this principle is enshrined in section 19 of the Criminal Code.

16. Greater difficulty is encountered where the mistake relates to the interpretation of a particular law, statutory or otherwise, or as to the existence of a right under the civil laws, for example, rights of property. This also qualifies as a mistake of law, but is it caught within the broad exclusionary principle contained in section 19 of the Code? It is in this area of what is loosely but compendiously referred to as "mistake of law" that confusion usually arises. We shall examine a series of situations in order to understand the true ambit of the "mistake of law" umbrella, which in one form or another has been relied upon by the R.C.M.P. in the belief that it excused or justified various activities that were subsequently called into question.

17. First, there are certain offences which by their very definition, including a requirement of *mens rea*, have traditionally been interpreted in such a way as to recognize a defence that is based on a mistake of law. Thus the offence of theft as defined in the Criminal Code (section 283) requires a fraudulent taking of the property of another without a colour of right. A long line of authorities has recognized that if an accused has a bona fide belief that he was

[14] *Pappajohn* v. *R.* (1980) 14 C.R. (3d) 243 at 267.

entitled to such property, even if his belief arises from a mistaken understanding of his rights under the law of property, he is not guilty of theft. The fact that his mistake is as to the law, and not as to the facts, does not preclude the accused from claiming that he was acting under a colour of right. The decision whether such a colour of right was honestly entertained in the circumstances is a question to be decided by the trier of fact, and what was said earlier on the subject of reasonableness applies equally to this kind of situation.

18. Second, it is far less certain that the principles will apply to those offences such as wilfully damaging the property of another, wilfully interfering with the enjoyment of another's property, arson or otherwise wilfully setting fire to property, which are contained in sections 387 to 402 of the Criminal Code. According to section 386 "No person shall be convicted of [any such] offence... where he proves that he acted with legal justification or excuse *and* with colour of right" (our emphasis). It might properly be argued that a bona fide mistake of law should entitle an accused person to claim that he was acting under a "colour of right", but this defence does not stand on its own, as in the case of theft. To a charge of arson or other wilful damage to property the defence must show both a "colour of right" and a "legal justification or excuse". Examples of the latter exemption from criminal liability or the even more familiar phrase "without lawful excuse" are numerous, whether the offence in question is contained in the Criminal Code or a federal or provincial statute. Irrespective of its source, the present legal position appears to leave no doubt that a mistake of law does not qualify as a "legal excuse" or "legal justification".

19. Third, we note the reservation expressed recently by one of Canada's foremost authorities on the criminal law. In *R.* v. *Walker and Somma*, Mr. Justice Martin of the Ontario Court of Appeal said:

> I would not wish to be taken to assent to the proposition that if a public official charged with responsibility in the matter led a defendant to believe that the act intended to be done was lawful, the defendant would not have a defence if he were subsequently charged under a regulatory statute with unlawfully doing that act.[15]

In principle, if the mistake of law arises from legal advice which is erroneous or is later held by a court to have been erroneous, there is still no defence. The reason, in part, is that it is undesirable to permit the definition of criminal conduct or of conduct giving rise to other offences to be dependent upon whether members of society can successfully shop around for a favourable legal opinion.[16] It may be assumed that even legal advice given by the Department of

[15] (1980) 51 C.C.C. (2d) 423 at 429.

[16] To the extent that the defence may exist, it is important that the efforts to ascertain the law be in good faith, which means by efforts which are as well designed to accomplish ascertainment as any available: see *Regina* v. *MacLean* (1974) 17 C.C.C. (2d) 84 at 106, per Judge O Hearn (Nova Scotia), quoting *Long* v. *State (Delaware)* (1949) 65 A. 2d 489. See Hall and Seligman, "Mistake of Law and *Mens Rea*" (1941) 8 *U. Chi. L. Rev.* 641 at 652; Arnold, "State-Induced Error of Law, Criminal Liability and *Dunn* v. *The Queen*: A Recent Non-Development in Criminal Law," (1978) 4 *Dal. L.J.* 559 at 579 *et seq.* Reliance on a lawyer's advice was rejected in *R.* v. *Brinkley* (1907) 12 C.C.C. 454 (Ont. C.A.) and *R. ex. rel. Irwin* v. *Dalley* (1957) 118 C.C.C. 116 (Ont. C.A.).

Justice to the R.C.M.P. that a practice is not criminal would not be recognized as the basis for a defence to a criminal charge, although there is no jurisprudence on the point. We think that the courts should be reluctant to permit such an exception. While the obtaining by the R.C.M.P. and the security intelligence agency of advice from the Department of Justice should be encouraged and facilitated, we do not think that such advice, if erroneous, should afford a defence to a charge. At most it should be considered as relevant to mitigation of sentence, and to the treatment of the offender within government. Any other approach would increase the tendency, which we have already observed, to seek an opinion from a higher level of the Department of Justice when the Department of Justice counsel assigned to the R.C.M.P. has given an opinion that the practice is unlawful.

20. Our view, that reliance on an official interpretation of the law ought not to be a defence, is contrary to that of the American Law Institute's *Model Penal Code* which allows a defence if the accused acts in reasonable reliance on

> . . . an official statement of the law, afterward determined to be invalid or erroneous contained in. . . an official interpretation of the public officer or body charged with responsibility for the interpretation, administration or enforcement of the law defining the offense.[17]

This proposed "official interpretation" defence assumes two things:

> . . . that the official is one to whom authority has been delegated to make pronouncements in a field of law, and that the authority can be held accountable by explicitly grounding it in the hands of an identifiable public official or agency. So grounded, the interest of both private citizens and government is served by protecting actions taken in reliance on that interpretative authority.[18]

Even if this defence were recognized by Canadian courts, we doubt that an opinion by some member of the Department of Justice, rather than the Attorney General himself, can properly be regarded as one by a public official who can be "held accountable".

21. A final point that might be argued related to mistake of law is that a policeman who commits an offence may have a defence if he believes that his superiors have obtained lawful authority to conduct the operation. In the Ellsberg break-in case, one of the judges held that because the "foot soldiers" who carried out the break-in were outsiders assisting an agent of the White House, they were entitled to act in objective good faith on the facts known to them:

---

[17] American Model Penal Code, Proposed Official Draft, section 2.04(3)(b)(iv).

[18] *United States* v. *Barker and Martinez* ("Barker II") (1976) 546 F. 2d 940, per Judge Leventhal (dissenting) at 957. This was the second *Barker* case. Barker and Martinez were the "foot soldiers" in the break-in at the office of the psychiatrist of Daniel Ellsberg, who had obtained the Pentagon papers. One of the majority judges, Judge Merhige, held that there was sufficient evidence of reliance on an official interpretation of the law that the defence of reliance on such a defence should have been submitted to the jury. The third member of the court, Judge Wilkey, approached the case without basing his judgment on this point.

> I think it plain that a citizen should have a legal defence to a criminal charge arising out of an unlawful arrest or search which he has aided in the reasonable belief that the individual who solicited his assistance was a duly authorized officer of the law.[19]

One commentator has written that the defence so stated "would seem to be a narrow one and inapplicable to a police officer".[20]

22. In addressing this problem it is well to remember what has been said already as to the dangers of considering the defence of mistake of law or mistake of fact in the abstract. Much depends on the definition of the particular offence. If the crime charged involves proof of *mens rea*, a policeman who mistakenly thinks that a warrant is in existence when in fact none exists, may have a defence based on a mistake of fact. The critical question then is whether the factual mistake negates the necessary mental element of the particular crime. Mistake of law presents a more difficult hurdle for the accused to get over. Even if the definition of the offence in question includes the element of "unlawfully" or "without lawful excuse or justification", the overwhelming body of Canadian and English case law denies to the accused a defence that rests on a mistaken belief that he had the necessary lawful authority to act as he did. Thus, an R.C.M.P. officer who acts in the mistaken belief that his superior possessed due lawful authorization to command the doing of certain acts, when in reality no such lawful authority is conferred by the law, is precluded from successfully invoking a mistake of law as his defence. If the principle tentatively expressed in *R.* v. *Walker and Somma* comes to be recognized, it will have to find its justification in some basis other than the defence of mistake.

(c) *Necessity*

23. In criminal law the Supreme Court of Canada has expressed a qualified acceptance of the defence of necessity. In *Morgentaler* v. *The Queen*, Mr. Justice Dickson, speaking for the majority of the Court, said that, if the defence does exist,

> . . . it can go no further than to justify non-compliance in urgent situations of clear and imminent peril when compliance with the law is demonstrably impossible. No system of positive law can recognize any principle which would entitle a person to violate the law because in his view the law conflicted with some higher social value.[21]

For the defence to be applicable, he said, the situation must be one of great urgency and the harm averted must be "out of all proportion to that actually caused by the defendant's conduct".

24. A situation in which the defence might arise is illustrated by an English case, *Johnson* v. *Phillips*, which held that a police constable in an emergency could violate a road traffic regulation without incurring a criminal penalty.

---

[19] *Ibid.*, at 954, per Judge Leventhal.

[20] M.L. Friedland, *National Security: The Legal Dimensions*, Ottawa, Department of Supply and Services, 1979, p. 103.

[21] (1975) 20 C.C.C. (2d) 449, at 497.

The court held that such action is justifiable if it is reasonably necessary for the protection of life or property. However the court emphasized the limits of the decision:

> No general discretion is given to a constable, even in cases where he himself considers that an emergency has arisen, to disobey traffic regulations or to direct other persons to disobey them.[22]

In other words, to use the language of Mr. Justice Dickson, the defence of necessity requires more than that the policeman himself thinks there is an emergency. There must in fact be an emergency, and in addition, the harm caused by violating the law must be less than the harm caused by not doing so.

25. Assuming, then, that the defence of necessity exists in Canadian criminal law, it becomes difficult to conceive of factual situations which have been placed before us in which the first test is satisfied — i.e. that there is an "urgent situation of clear and imminent peril". That test is certainly not satisfied by a perception, even if accurate, that in a vague and general sense Canadian society was faced with an emergency — or a "state of war", as Commissioner Higgitt described the situation confronting the R.C.M.P. in 1971-72. Nor is the second test satisfied. At most it can be said that in criminal investigations and the peace officer's role in the prevention of crime, the defence may stand against charges of breaking and entry and of violation of traffic laws. We refer to this further in Part III, Chapters 2 and 8.

26. Before leaving necessity as a defence, we should note that it may also be a defence if a policeman is sued for damages for a wrongful act. As far as the common law of tort is concerned, the extent to which the defence exists at all is unclear. One textwriter, in discussing necessity as a defence, says:

> The defence, if it exists, enables a defendant to escape liability for the intentional interference with the security of another's person or property on the ground that the acts complained of were necessary to prevent greater damage to the commonwealth or to another or to the defendant himself, or to their or his property... There is some authority that the subject as well as the Crown has a right and a duty at common law to justify a trespass or other tort on the ground of necessity in the defence of the realm, but such a right has been said to be obsolescent.[23]

The textwriters appear to agree that, if the defence exists, it cannot be relied upon unless there is a real and imminent danger.[24] As one writer says, "Only an urgent situation of imminent peril can ever raise the defence, lest necessity become simply a mask for anarchy".[25] This must be true whether the defendant is a private citizen or a policeman. Necessity, described by Milton as "the tyrant's plea", has not been accepted as a ground for action by the state that would otherwise be a tort. Ever since the case of *Entick* v. *Carrington* (see Part III, Chapter 2), it has been accepted that necessity "for the ends of govern-

---

[22] *Johnson* v. *Phillips* [1975] 3 All E.R. 682, at 685, per Mr. Justice Wien.

[23] *Salmond on Torts*, 16th ed. 1973 (ed. Heuston) p. 504.

[24] *Salmond on Torts*, 16th ed. 1973, p. 505; *Winfield and Jolowicz on Tort*, 10th ed. 1975, p. 635.

[25] Fleming, *The Law of Torts*, 5th ed. 1977, p. 94.

ment" — "state necessity" — is not a defence recognized by the common law. However, it should be noted that the question there was not one involving an urgent situation of imminent physical peril to any person or property.

(d) *Duress*

27. Unlike necessity, with respect to which the Canadian Criminal Code makes no express provision, the plea of duress is principally governed by section 17 of the Code which states:

> A person who commits an offence under compulsion by threats of immediate death or grievous bodily harm from a person who is present when the offence is committed is excused for committing the offence if he believes that the threats will be carried out and if he is not a party to a conspiracy or association whereby he is subject to compulsion, but this section does not apply where the offence that is committed is high treason or treason, murder, piracy, attempted murder, assisting in rape, forcible abduction, robbery, causing bodily harm or arson.[26]

When duress is pleaded, it is claimed that the wrong was committed in order to prevent harm to the accused or another person. The basis of the defence is not that the threat of immediate death or serious bodily injury is such as to destroy or neutralize the accused's will, nor indeed that it demonstrates the accused had no *mens rea*. Rather it is an acknowledgment of and a concession to human weakness. The law recognizes that in the face of an overwhelming threat of grave personal injury it cannot expect extraordinary standards of resistance.

28. Until lately, it had been thought that the above quoted section in the Criminal Code contained the all-embracing conditions of which the defence of duress must be judged in a criminal case. This is no longer so, following the decision of the Supreme Court of Canada in *R.* v. *Paquette*[27] which held that the restrictive terms of section 17 do not govern the situation where the accused is charged with aiding and abetting rather than being the principal offender who actually commits the crime in question. In the opinion of the Supreme Court section 17 codifies the law as an excuse for the actual commission of the crime but, by its very terms, it does not go beyond that. Should the accused therefore be faced with a charge of aiding or abetting he can invoke instead the defence of common law duress. After remaining static for several centuries this branch of the criminal law has been the focus of much attention in recent years by the English courts, culminating in the decision of the House of Lords in *Lynch* v. *D.P.P. of Northern Ireland*,[28] that the defence of duress is available even with respect to the crime of murder, at least if the charge is one of aiding and abetting. As for the other ingredients of the defence, e.g., the nature of the threats, there is no indication as yet that the common law principles will be relaxed. It can, however, be said that the whole

---

[26] For a full discussion of this defence, see Mewett and Manning, *Criminal Law*, Toronto, Butterworths, 1978, pp. 245 *et seq.*

[27] [1977] 2 S.C.R. 189.

[28] [1975] 1 All E.R. 913.

tenor of the most recent jurisprudence is towards a relaxation of the previously severe qualifying conditions of this defence.

29. What relevance then does the law of duress have towards the activities of members of the R.C.M.P. or of a security intelligence agency? As in the case of necessity it is difficult for us to imagine how the defence of duress would be applicable to any of the practices or factual situations involving the R.C.M.P. which have come to our attention. At most one could envisage the possibility of its application of an undercover operative who has penetrated a violence-prone group, whose true identity is suspected by the members of the group, and who is threatened with bodily harm if he does not participate in some act of violence. Such participation, it must be recognized, may take several forms ranging from merely facilitating the commission of the crime by others (e.g., driving the members of the violent group to the scene of the crime) to the actual perpetrating of the crime itself (e.g. setting fire to property or inflicting blows upon another). Furthermore, the amount of prior warning that a serious crime is planned by the group and that some degree of participation by the undercover operative is expected may vary according to the circumstances. It would be wrong to conclude that the situations revealed to us are necessarily conclusive as to the possible future eventualities that might befall undercover operatives of the R.C.M.P. or the security intelligence agency.

30. It is clear, both in the common law and section 17 versions of the defence of duress, that a person who, with knowledge of its nature, joins a criminal association which he realizes might bring pressure upon him to commit an offence, should normally not be entitled to avail himself of the defence. Nevertheless, it could be argued that the position of a police undercover operative is essentially different from that of an ordinary person. This argument commended itself to the English Law Commission which in its report to Parliament on the future law of duress stated[29]

> There may also be cases where a person, employed... by the police to infiltrate a ring of drug smugglers or to seek out information about an illegal organization, has to put himself in a situation in which he knows that he may be subjected to duress because of his activities. It would be wrong to deny him the defence in these circumstances, and for that reason we think that the defence should be excluded only where the person has acted without reasonable cause in putting himself in that situation.

31. The dilemma facing the undercover operative as to whether he should escape or not may vary in degrees of intensity, dependent upon the immediacy of the threats and the serious nature of the dangers to the lives of innocent people represented by the violence-prone group which has been infiltrated. Faced with the choice between personally engaging in the criminal activities of the group or dissociating himself from such activities, we think that the undercover operative should withdraw from the group. At the same time we are realistic enough to envisage extraordinary situations arising in the future for which provision must be made in the relevant law of duress. With one significant change we agree with the recommendation of the English Law

[29] *Law. Com.*, No. 83, p. 13.

Commissioners and exclude the availability of the defence where the undercover operative has acted without sufficient and reasonable cause in either (1) putting himself in the situation where threats to his life or person are to be expected or (2) remaining in such a situation. The burden of establishing the defence would remain upon the accused.

B. LACK OF EVIL INTENT

32. It has been contended by counsel for the R.C.M.P. that no criminal offence is committed by a member of the R.C.M.P. unless he has evil intention, or a "vicious will". Counsel for the R.C.M.P. place great stress, in support of this argument, on the following passage from the reasons for the judgment of the Supreme Court of Canada, delivered by Mr. Justice Dickson, in *Regina* v. *Sault Ste. Marie*:

> The doctrine of the guilty mind expressed in terms of intention or recklessness, but not negligence, is at the foundation of the law of crimes. In the case of true crimes, there is a presumption that a person should not be held liable for the wrongfulness of his act if that act is without *mens rea*. Blackstone made the point over two hundred years ago in words still apt: "to constitute a crime against human laws, there must be, first, a vicious will; and secondly, an unlawful act consequent upon such vicious will"... See *Commentaries on the Laws of England* (1809) Book IV, 15th ed., c. 15, p. 21. I would emphasize at the outset that nothing in the discussion which follows is intended to dilute or erode that basic principle.[30]

33. The judgment as a whole does not suggest that the Supreme Court of Canada requires proof of a "vicious will" for a conviction in criminal cases.[31] Mr. Justice Dickson quoted Blackstone to make the point that the facts of the *Sault Ste. Marie* case did not concern a "true crime" but rather regulatory offences. At a later point in the judgment he stated the principle which our courts have followed:

> Where the offence is criminal, the Crown must establish a mental element, namely, that the accused who committed the prohibited act did so intentionally or recklessly, with knowledge of the facts constituting the offence, or with wilful blindness toward them.

It will be noted that in that statement he makes no mention of evil intent or "vicious will". This is not surprising, for any requirement that "vicious will" be present for a crime to be committed would introduce a fundamental change in Canadian criminal law, and if that were intended we would have expected that the Court's intention to do so would have been more clearly stated.

34. The text writers have stated the accepted law without reference to such a requirement. Indeed, on the contrary, the law has rejected such a requirement. One leading text says:

---

[30] (1978) 40 C.C.C. (2d) 353 at pp. 357-8.

[31] The actual decision in the case was that in regard to crimes of strict liability in which the definition of the offence does not refer to or require a guilty mind, the absence of negligence (or the presence of due diligence in an attempt to avoid the conduct complained of) is a relevant factor when considering liability.

> *Mens rea* refers to the mental element required for many crimes. It must not be read in its literal sense as requiring moral wrong or dishonest intent or conscious guilt. A person who breaks the law with a good motive, or for conscientious reasons, or from religious belief, still commits a crime. So also (in many cases) does a person who breaks the law in justifiable ignorance of its existence, and with no intention of committing even a moral wrong.[32]

Another text book says:

> *Mens rea* is a technical term. It is often loosely translated as 'a guilty mind', but this translation is frequently misleading. A man may have *mens rea*, as it is generally understood today, without any feeling of guilt on his part. He may, indeed, be acting with a perfectly clear conscience, believing his act to be morally, and even legally, right, and yet be held to have *mens rea*.[33]

35. It is true that in scattered cases in the nineteenth and twentieth centuries there have been judicial statements similar to Blackstone's — phrases such as 'an evil mind with regard to that which he is doing', 'a bad mind', or references to acts done not 'merely unguardedly or accidentally, without any evil mind'.[34] As Professor H.L.A. Hart has written:[35]

> Some of these well-known formulations were perhaps careless statements of the quite different principle that *mens rea* is an intention to commit an act that is wrong in the sense of legally forbidden. But the same view has been reasserted in general terms in England by Lord Justice Denning: 'In order that an act should be punishable, it must be morally blameworthy. It must be a sin.'[36] Most English lawyers would however now agree with Sir James Fitzjames Stephen that the expression *mens rea* is unfortunate, though too firmly established to be expelled, just because it misleadingly suggests that, in general, moral culpability is essential to a crime, and they would assent to the criticism expressed by a later judge that the true translation of *mens rea* is 'an intention to do the act which is made penal by statute or by the common law'.[37]

Professor Hart also pointed out that the use of language such as Blackstone's, excluding liability in the absence of fault or 'moral wrong'

> . . . may have blurred the important distinction between the assertion that (1) it is morally permissible to punish only voluntary action and (2) it is

---

[32] Glanville Williams, *Textbook of Criminal Law*, London, Stevens, 1978, at pp. 49-50. See *Proprietory Articles Trade Association* v. *Attorney General for Canada* [1931] A.C. 310 at 324, where Lord Atkin distinguished between morality and the criminal quality of an act, the latter being judged by whether the act is prohibited with legal consequences.

[33] Smith and Hogan, *Criminal Law*, 4th ed., London, Butterworths, 1978, at p. 47.

[34] Lord Esher in *Lee* v. *Dangar* [1892] 2 Q.B. 337.

[35] H.L.A. Hart, *Punishment and Responsibility*, Oxford, Clarendon Press, 1968, at p. 36.

[36] Sir Alfred Denning, *The Changing Law*, London, Stevens, 1953, p. 112.

[37] *Allard* v. *Selfridge* [1925] 1 K.B. at 137, per Mr. Justice Shearman. Hart notes that when quoting this passage in *Criminal Law: The General Part* (2nd ed.), p. 31, Glanville Williams commented that the judge should have added 'or recklessness'.

morally permissible to punish only voluntary commission of a moral wrong.[38]

36. In conclusion, we reject the general contention that the Supreme Court of Canada has made it the law of Canada that the absence of an evil mind is a defence by way of negativing *mens rea*.

C. INTERPRETATION ACT, SECTION 26(2)

37. The R.C.M.P. has advanced as a general defence for the conduct of its members, when they are authorized to do something specific, section 26(2) of the Interpretation Act.[39] This has been put forward particularly in connection with the subject of electronic surveillance. Section 26(2) provides:

> Where power is given to a person, officer or functionary, to do or enforce the doing of any act or thing, all such powers shall be deemed to be also given as are necessary to enable the person, officer or functionary to do or enforce the doing of the act or thing.

In Part III, Chapter 3 we discussed whether section 26(2) is authority for concluding that when a judge grants an authorization under section 178.13 of the Criminal Code for electronic eavesdropping by microphone, or the Solicitor General issues a warrant for the same purpose under section 16 of the Official Secrets Act, there is an implied power of entry to effect the installation. Our opinion, expressed in that chapter, is that section 26(2) does not provide such authority.

38. Here we need say no more than that section 26(2) cannot, in our opinion, in general be relied upon as a defence where the act is otherwise unlawful. In the absence of *express* words permitting the subsection to be construed as granting not only lawful ancillary powers but also otherwise unlawful ones, we cannot accept a construction of the statute that would countenance such a result. The courts have traditionally presumed that a statute does not abridge common law rights, and that such abridgement can occur only by the use of express words or as a matter of "plain implication".[40] The argument has been advanced on behalf of the R.C.M.P. that the implied powers provided for in section 26(2) may be relied upon as a defence, generally, when methods otherwise unlawful, are used in the course of operations within the scope of the duties of a peace officer and reasonably necessary for their execution.

---

[38] H.L.A. Hart, *Punishment and Responsibility*, Oxford, Clarendon Press, 1968, at p. 40.

[39] R.S.C. 1970 ch. I-23.

[40] See Maxwell, *Interpretation of Statutes*, 12th ed., London, Sweet and Maxwell, 1969, at p. 116; *Manitoba Government Employees Association* v. *Government of Manitoba* [1977] 5 W.W.R. 247 at 258 (Supreme Court of Canada). See also *Attorney General for Canada* v. *Hallett & Carey Ltd.* [1952] A.C. 427 at 450-1 (P.C.); *Board of Commissioners of Public Utilities* v. *Nova Scotia Power Corporation* (1976) 18 N.S.R. (2d) 692 at 709-11 (N.S.C.A.); *Fullerton* v. *North Melbourne Electric Tramway and Lighting Co. Ltd.* (1916) 21 C.L.R. 181; *Quebec Railway, Light, Heat and Power Company* v. *Vaudry* [1920] A.C. 662 at 679-80 (P.C.).

39. Even if section 26(2) were available as a defence, it must be remembered that powers must not be implied unless the powers expressly granted by the statute in question "cannot otherwise be reasonably and effectively exercised" without the powers sought to be added by implication. The statutory provision does not alter the power to imply ancillary powers that the courts had at common law, nor does it extend the right to imply such powers.[41] Moreover, the word "necessary" in section 26(2) is to be distinguished from such words as "beneficial", "desirable" or "convenient" which are not found in the subsection.[42] The notion of necessity, in contrast with the other words just mentioned, is interpreted by the courts as meaning that the absence of the power sought to be implied would defeat either the purpose for which the statute was enacted or the express powers conferred by the statute.[43]

D. CRIMINAL CODE, SECTION 25(1) — "PROTECTION OF PERSONS ACTING UNDER AUTHORITY"

40. The R.C.M.P. has also submitted that section 25(1) of the Criminal Code provides a broad legal justification for conduct which would otherwise be unlawful. Section 25(1) provides:

> 25. (1) Every one who is required or authorized by law to do anything in the administration or enforcement of the law
>
> (a) as a private person,
>
> (b) as a peace officer or public officer,
>
> (c) in aid of a peace officer or public officer, or
>
> (d) by virtue of his office,
>
> is, if he acts on reasonable and probable grounds, justified in doing what he is required or authorized to do and in using as much force as is necessary for that purpose.

41. We have already discussed this provision when we considered, in Part III, Chapter 3, whether it justifies an implied power of entry to install electronic eavesdropping devices. But of course the section is of broader relevance. Indeed, counsel for the R.C.M.P. has submitted that this section "affords a valid defence to a member of the R.C.M.P., as a peace officer, in the context of a prosecution arising out of any reasonably necessary act committed by the member while acting in execution of a lawfully imposed duty". However, this statement of the scope of section 25(1) does not include all three of the essential ingredients of the defence that may be founded on the section:

---

[41] *Township of Nelson*, v. Stoneham (1957) 7 D.L.R. (2d) 39 at 42-3 (Ont. C.A.).

[42] *H.P. Bukner Ltd.* v. *J. Bellinger S.A.* [1974] Ch. 401 (English C.A.). At p. 423, Lord Denning M.R. said that the word "necessary" is "much stronger than 'desirable' or 'convenient'". See also *In re The Haggert Brothers Manufacturing Company (Limited)* (1893) 20 Ont. A.R. 597 at 602.

[43] *Interprovincial Pipeline Ltd.* v. *National Energy Board* (1977) 17 N.R. 56 (Fed. C.A.).

(a) The peace officer must be acting in his capacity as a peace officer or, to use the more familiar phraseology, acting in the execution of his duties as a peace officer.

(b) The act in question — the act alleged to be unlawful and in breach of the criminal law or civil law — must be some act which the police officer is required or authorized by law to do in the course of the administration or enforcement of the law.

(c) There must be reasonable and probable grounds upon which the police officer claims (i) that his legally authorized actions were justified in the circumstance, and (ii) where appropriate, that the amount of force used was necessary in the circumstances.

It is the second of these requirements that fails to find a place in the formulation by counsel for the R.C.M.P. The importance of this requirement was emphasized by Mr. Justice Dickson in *Eccles* v. *Bourque*,[44] in a passage that we quoted from in Part III, Chapter 3, and with which we agree. Before the statutory protection can be relied upon, the act in question must be one which the policeman is required or authorized by law to do, and it is inaccurate and misleading to say that it is sufficient that the member was acting in execution of a "lawfully imposed duty".[45] This point was clearly stated by Judge Zalev of the County Court of Ontario in *R.* v. *Walker*.[46] In that case the accused was a police officer. He was charged with failing to stop at a stop sign. He had driven one of two police vehicles that had been dispatched to a bank because of a possible robbery. On approaching an intersection his emergency lights were flashing and he slowed to about 10 m.p.h., but he did not stop at the stop sign. His vehicle collided with another car in the intersection. The police officer was convicted at trial, and, on appeal, Judge Zalev upheld the conviction. He held that the defence of necessity did not apply, and he rejected a defence based on section 25(1). He adopted the reasoning of Mr. Justice Dickson in *Eccles* v. *Bourque* and properly posed the central question raised by the facts of the case as follows:

> . . . the question which must be answered in this case. . . is not whether the appellant was required to answer the call to the bank without delay, but whether the appellant was required or authorized by law to drive past a stop sign without stopping.

There being no specific provision in the Ontario Highway Traffic Act which requires or authorizes a police officer to ignore a stop sign, it became necessary to consider whether any common law protection could be invoked so as to bring the provisions of section 25(1) into play. He therefore discussed *Johnson* v. *Phillips*, an English case which we have already referred to.[47] As we understand Judge Zalev's conclusion, it is that while at common law the circumstances may afford a defence of necessity, the same circumstances would not

---

[44] (1974) 19 C.C.C. (2) at pp. 130-31.

[45] Neither of the authorities cited by counsel for the R.C.M.P. (*R.* v. *Redshaw* (1975) 31 C.R.N.S. 225; *R.* v. *Walker* (1979) 48 C.C.C. (2d) 126) provides support for the interpretation of section 25(1) urged by counsel for the R.C.M.P.

[46] (1979) 48 C.C.C. (2d) 126.

[47] [1975] 3 All E.R. 682 (Divisional Court). See footnote 22.

support a defence under section 25(1). We consider that conclusion to be an accurate statement of the law.

42. There are two further submissions made by counsel for the R.C.M.P. in regard to section 25(1) which we feel obliged to comment upon. One is that "section 25 affords a member of the R.C.M.P., as a peace officer, a valid defence to a prosecution in respect of acts that he was ordered to commit by a person who had the jurisdiction, or the colour of jurisdiction, to make such an order". This proposition is cited in Taschereau's 1893 edition of the Criminal Code.[48] However, a reading of what was said there makes it clear that what was envisaged was the kind of situation covered by section 25(2) of the Code (justification for a person required or authorized by law to execute a process or carry out a sentence, or for another person assisting him, even if the process or sentence is defective or made without jurisdiction) — and has nothing to do with section 25(1).

43. The other submission is that "a member of the R.C.M.P., as a peace officer, who acts in the honest belief that he was authorized to do what he did under the circumstances, where that belief was reasonable on the facts of the particular case, is entitled to assert the section 25 defence...". We disagree. The honesty or genuineness of the peace officer's beliefs is irrelevant where, as stated in section 25(1), the governing criterion is whether there are reasonable and probable grounds to support the police officer's claim that his legally authorized acts were justified in the circumstances, and whether there are reasonable and probable grounds for using the force which he used. The test in both instances is objective, not subjective; the issues involved in section 25(1) have nothing to do with the state of mind of the peace officer.

E. IMMUNITIES

44. In this section we shall consider the extent to which members of the R.C.M.P., acting in the course of their duty, are protected by some ground of immunity from successful prosecution for violation of federal statutes (such as the Criminal Code) or provincial statutes that impose penalties (such as the Highway Traffic Acts). There are four possible grounds on which immunity might be argued. Each of them will be discussed in turn. They are as follows:

(a) Crown immunity

(b) Intergovernmental immunity

(c) Exclusive power (interjurisdictional) immunity

(d) Immunity as a result of the paramountcy of the R.C.M.P. Act

Counsel for the R.C.M.P. has suggested that, if individual members of the R.C.M.P. were prosecuted for federal or provincial offences, they might raise a defence based on one or more of the foregoing if their acts in question were "reasonably necessary for the effective performance of their duties". This argument, if valid, would apply to a far broader range of factual situations

[48] As quoted in *Crankshaw's Criminal Code* (8th ed., 1979), at 1-133.

than would support the defence of necessity, which is discussed elsewhere in this Part.

45. Our analysis of this issue must be largely on principle and by reference to cases that do not decide the application or non-application of principle to the R.C.M.P. There is a paucity of reported cases in which members of the R.C.M.P. have been subject to prosecution under federal or provincial laws in regard to their actions carried out in the course of their duties; and no reported cases in which these grounds have been raised as a defence and considered by the court.

46. When we refer to provincial laws, we must be understood to include municipal by-laws, which depend on provincial legislation for their authority and validity. In the case of municipalities within Territories, their status depends on legislation enacted by the Parliament of Canada.

(a) *Crown immunity*

47. It has been submitted to us by counsel for the R.C.M.P. that members of the R.C.M.P. are servants of the Crown and as such enjoy the benefit of the immunity of the Crown itself from prosecution even under federal laws such as the Criminal Code. It was conceded that members of the R.C.M.P., while performing law enforcement functions, might be liable to prosecution under federal criminal law (but not under provincial law because of additional arguments advanced under later headings) because their functions and duties are similar to those of any peace officer or constable, rather than being uniquely Crown functions or duties. In other words their extensive discretionary powers may disentitle them to the status (and immunity) of an agent or servant of the Crown. On the other hand, according to the submission of counsel for the R.C.M.P., because members of the R.C.M.P. performing national security functions are exercising more restricted discretionary powers, they engage in federal Crown activities and may be immune from prosecution in the Courts for reasonably necessary acts committed in the course of their duties. Their accountability, so it is contended, is to the Commissioner of the R.C.M.P. and to the Solicitor General of Canada, not to the courts.

48. It is undoubtedly true that at common law the Crown enjoys an immunity from prosecution for a statutory offence unless the statute creating the offence expressly states that the Crown is to be bound. The common law rule is embraced by both federal and provincial legislation as to the interpretation of statutes. Thus, for example, the federal Interpretation Act provides:

> 16. No enactment is binding on Her Majesty or affects Her Majesty or Her Majesty's rights or prerogatives in any manner, except as therein mentioned or referred to.[49]

[49] The statutory rule does not leave any room for a statute to bind the Crown by necessary implication, as had been possible under the common law formulation of the prerogative's effect: *Her Majesty the Queen in the Right of the Province of Alberta* v. *Canadian Transport Commission* [1978] 1 S.C.R. 61.

Therefore, in order to restrict the Crown, a federal enactment must be very specific in indicating that such an effect is intended.

49. The Supreme Court of Canada has held that the Criminal Code falls short of meeting this requirement: though the code includes the Crown in its definition of "person", a word used by the Code generally to refer to both offenders and victims of criminal conduct, the reference to the Crown is only to the Crown as victim rather than as wrongdoer.[50] Consequently, the Crown cannot be guilty of committing a Criminal Code offence and is, in effect, immune from prosecution for such an offence.

50. The rule of immunity from statute, in its prerogative or provincial statutory form, has been taken to afford immunity to the federal Crown from provincial statutes which do not specifically include the Crown.[51] Consequently the federal Crown enjoys a substantially similar degree of immunity from provincial legislation as it does from federal legislation, such as the Criminal Code, as a matter of construction of the relevant legislation.

51. The benefit of immunity from statute accrues not only to the Crown (in a practical sense — the government) but to servants and agents and others acting on behalf of the Crown, if the Crown would be detrimentally affected by prosecution. Thus in *Canadian Broadcasting Corporation* v. *Attorney General of Ontario* the Canadian Broadcasting Corporation (the C.B.C.), a federal Crown agency, was held to be free of any liability for broadcasting on Sunday contrary to the general prohibitions of the Lord's Day Act (Canada).[52] However, in an even more recent decision involving the C.B.C.,[53] the Ontario Court of Appeal held the C.B.C. liable to prosecution for broadcasting an obscene film contrary to section 159 of the Criminal Code because in so doing it was acting outside the scope of its statutory authority. This was particularly evident because the Regulations under the Broadcasting Act (Canada), to which the C.B.C. is subject, specifically prohibit the broadcast of anything contrary to law or any obscene, indecent or profane language or pictorial presentation.

52. Counsel for the R.C.M.P. argues that R.C.M.P. personnel, when acting in the course of duty, are agents of the federal Crown and therefore enjoy the same immunity as the Crown. It is at this point that the argument based on Crown immunity breaks down, since in our view, even if members of the R.C.M.P. are agents or servants of the Crown, it is only if contravention of the

---

[50] See *Canadian Broadcasting Corporation* v. *Attorney General of Ontario* [1959] S.C.R. 188. It is true that what was being interpreted in this case was the Lord's Day Act, not the Criminal Code. However, the Lord's Day Act incorporates the Code's definition of "person".

[51] See, for example, *R.* v. *Sanford* [1939] 1 D.L.R. 374 (N.S.S.C. in banco). There are numerous cases on this point, which are collected in McNairn, *Governmental and Intergovernmental Immunity in Australia and Canada*, Toronto and Buffalo, University of Toronto Press, 1977, at p. 24, n.3.

[52] *Canadian Broadcasting Corporation* v. *Attorney General of Ontario* [1959] S.C.R. 188.

[53] *R.* v. *C.B.C.* (1980) 16 C.R. (3d) 78 (Ont. C.A.).

law were unavoidable in the course of carrying out their duties that it could be said that they could enjoy the protection of Crown immunity.

53. Let us first ask whether the R.C.M.P. itself is an agent of the Crown. If it is not, then *a fortiori* its members are not agents or servants of the Crown. If it is, however, it does not automatically follow that its members are entitled to rely on Crown immunity.

54. Is the R.C.M.P. itself an agent of the Crown? The general principle upon which courts determine whether an individual or organization is a Crown agent is as follows:

> Whether or not a particular body is an agent of the Crown depends upon the nature and degree of control which the Crown exercises over it.[54]

A Crown agency is "a body which is subject at every turn in executing its powers to the control of the Crown".[55] Whether the R.C.M.P. is subject to that degree of control will depend very much upon the meaning of section 5 of the R.C.M.P. Act. In Part X, Chapter 4 we point out how ambiguous that section is. There is no need to repeat here what we there observe; the most we can say is that the ambiguity of the section makes it likely that the section alone cannot be regarded as the foundation for a proposition that members of the R.C.M.P. lack the traditional characteristics of constables. The characteristics that we refer to are those which leave the constables free from direct control in the exercise of their powers of investigation, arrest and initiation of prosecutions.

55. Suffice to say that the R.C.M.P. may not be a Crown agent. If it is not, R.C.M.P. personnel would not be able to claim Crown immunity from either federal or provincial laws. Yet, there is some implied support to be found in the R.C.M.P. Act for the proposition that members of the R.C.M.P. are agents or servants of the Crown. It is true that section 53 of the R.C.M.P. Act and section 37 of the Federal Court Act (Canada) specifically deem members of the Force to be servants of the Crown "for the purpose of determining liability in any action or other proceeding by or against the Crown". But those provisions appear on a strict reading to be referring to civil rather than criminal proceedings. The expression "proceedings by or against the Crown" is particularly apt to describe civil claims made by or initiated against the federal Crown and does not easily fit the situation of a criminal proceeding against a federal Crown servant. The proceedings by and against the Crown with which the Federal Court Act deals are restricted to civil proceedings. It would be logical to read section 53 of the R.C.M.P. Act in the same sense as the comparable section of the Federal Court Act unless there is something in the context of the former Act which clearly dictates another conclusion. The R.C.M.P. Act does not in fact contain any language which suggests that the larger meaning, embracing criminal proceedings, was intended in the deeming provision of that Act.

---

[54] *Westeel-Rosco Ltd.* v. *Board of Governors of Smith Saskatchewan Hospital Centre* (1976) 69 D.L.R. (3d) 334, at 342-3, per Mr. Justice Ritchie. More recently, see *Fidelity Insurance Co.* v. *Workers Compensation Board* (1980) 102 D.L.R. (3d) 255.

[55] Per Mr. Justice Ritchie in the *Westeel-Rosco* case, *Ibid.*, at 343.

56. Moreover, the provisions in the R.C.M.P. Act and the Federal Court Act create a master-servant relationship for two purposes only: liability to the Crown and liability of the Crown. They have no application to situations in which what is involved is the personal liability of the R.C.M.P. member. In conclusion, these sections do not assist in determining the status of a member of the R.C.M.P. in criminal proceedings. It may be, however, that the provisions of the R.C.M.P. Act, considered as a whole, support the conclusion that a member of the Force is a Crown servant for all purposes, including that of determining personal criminal liability.[56]

57. It does not follow that R.C.M.P. members, even if they are agents or servants of the Crown, are entitled to rely on Crown immunity. The immunity which they would be entitled to enjoy would not be absolute. It would have to be established in the particular case that the Crown would be prejudiced in some significant way by making the servant or agent subject to the prohibition contained in the statute. The decision in *R.* v. *Stradiotto*[57] makes this clear. In that case a member of the Canadian Armed Forces, who was driving an army truck in the course of his duties when the truck was involved in a serious traffic accident, was charged with an offence under the provincial Highway Traffic Act. The Ontario Court of Appeal held that he was not immune from prosecution under the provincial Act even though the legislation did not specifically refer to the Crown. The Court pointed out that it is only the Crown itself which is immune from legislation, not its servants and agents; the immunity is applicable to servants and agents only to the extent that Crown rights would be prejudiced if the servants or agents were subject to the legislation. Thus, it was observed in the *Stradiotto* case, army personnel are not required to have provincial drivers' licences in order to drive military vehicles within a province, because such a requirement would interfere with the right of the federal Crown to operate military vehicles in the province.[58] The immunity has been held to apply where, although unlicensed, the servicemen's duties or superior orders have necessitated that they drive government vehicles in the course of their military service.[59] If, on the other hand, it is possible for a servant or agent of the Crown to carry out his or her orders without contravening the provincial law, as was the situation in the *Stradiotto* case, the servant or agent is not immune from the law in question. Since the military driver in *Stradiotto* did not have to drive negligently or unlawfully in order to perform his duty, he was held to be subject to the provincial Highway Traffic Act. Indeed, in other cases servicemen have been held liable for highway traffic violations such as careless or unsafe driving.[60] Liability in that situation does

---

[56] This cannot be stated with conviction, for it requires an inference that the statute by implication deviates from the traditional principle that police officers are independent public officers rather than servants or agents of those who pay their salaries. For the latter principle, see *McCleave* v. *Moncton* (1902) 32 S.C.R. 106.

[57] [1973] 2 O.R. 375.

[58] Citing *R.* v. *Rhodes* [1934] O.R. 44.

[59] See *R.* v. *Henderson* [1930] 2 W.W.R. 595, and *R.* v. *Rhodes* [1934] 1 D.L.R. 251 (Ont. S.C.).

[60] See also *R.* v. *McLeod* [1930] 4 D.L.R. 226 (N.S.S.C. in banco) (serviceman guilty of reckless driving).

not interfere with the right of the Crown to direct the activities of its servant for normal Crown purposes. The R.C.M.P. has received legal advice that the case of *Stradiotto* is authority for the proposition that members of the R.C.M.P. do not break the traffic law if members are doing that which is reasonably necessary for the carrying out of the duties and responsibilities assigned to them by or under federal legislation. We do not think that the case is authority for that view. We consider that the decision in *Stradiotto*, which may support the conclusion that there is immunity when the member is carrying out a specific order and he cannot do so otherwise than by violating the traffic law, does not provide support for a similar conclusion when the member is merely carrying out his duties in a general sense.

58. Applying these principles to the R.C.M.P., we conclude that even if members of the R.C.M.P. are agents or servants of the Crown, they will be bound by provincial or federal laws while carrying out their duties, except to the extent that non-compliance is unavoidable in the sense that they were specifically directed to carry out the very conduct which is in question. In other words, even if his actions are in the course of duty, a member of the R.C.M.P. would be subject to successful prosecution for actions which violated a federal or provincial statute and which he was not specifically directed to carry out. It is at the very least doubtful that the member could successfully establish immunity on the basis that what he did was "reasonably necessary" to the performance of his duties, though not the subject of specific directions.

59. As a general rule, peace officers are subject to the criminal law except to the extent that specific statutory protection is afforded to them. As Mr. Justice Laskin said when he was a member of the Ontario Court of Appeal:

> In principle, the recognition of "public duty" to excuse breach of the criminal law by a policeman would involve a drastic departure from constitutional precepts that do not recognize official immunity, unless statute so prescribes... Legal immunity from prosecution for breaches of the law by the very persons charged with a public duty of enforcement would subvert the public duty...
>
> The Criminal Code presently prescribes justification for policemen and others in a number of respects where they are proceeding to enforce the law, as, for example, by arresting offenders. This is designed as an aid to enforcement, and presumes that the enforcing officers are not themselves participating in the criminal activity that they are seeking to curb. Recognition of "legal lawlessness" is, however, something far different. It does not represent a value that fits into our system of criminal law...[61]

More recently and briefly, in the context of a case concerning the use of police informers, Chief Justice Laskin has said:

> The police, or the *agent provocateur* or the informer or the decoy used by the police do not have immunity if their conduct in the encouragement of a commission of a crime by another is itself criminal.[62]

---

[61] *R.* v. *Ormerod* [1969] 2 O.R. 230 at 244-5 (Ont. C.A.).

[62] *Kirzner* v. *The Queen* [1978] 2 S.C.R. 487 at 491. See also *Attorney General of Quebec and Keable* v. *Attorney General of Canada et al* [1979] 1 S.C.R. 218 at 242, where Mr. Justice Pigeon said that members of the R.C.M.P. "enjoy no immunity from the criminal law".

60. In light of that principle, a criminal court would be unlikely to allow a peace officer, even if he is a servant or agent of the Crown, much latitude to rely on "reasonable necessity" unless a statute permitted it as a defence.

61. There is another point to be made, which seems to preclude the availability of Crown immunity to a member of the R.C.M.P. Section 25 of the Regulations under the R.C.M.P. Act imposes upon every officer and every person in charge of a post the duty and responsibility of ensuring "at all times strict observance of the law..." by all members of the Force. It may be argued, then, that each member of the Force should be taken to assume that orders given to him are to be carried out in accordance with the law.[63] However, if those orders were to direct clearly a breach of the law or could be carried out only by violating the law, then it may be that the superior from whom the orders originated would be liable on the basis that his discretionary authority did not extend to authorizing breaches of the law. If the orders emanated in the first instance from an officer, as defined in section 6 of the R.C.M.P. Act, or a person in charge of a post, then that individual would be in much the same position as the C.B.C. in the second C.B.C. case.[64] He would have exceeded a requirement to ensure compliance with the law contained in regulations governing his behaviour and should, accordingly, be subject to prosecution for his criminal conduct.

62. There is no general rule that peace officers are not subject to criminal liability because of the large degree of discretion entrusted to them. There is authority for the proposition that no superior authority is responsible for the tortious acts of a policeman or other public office holder who is exercising a discretionary power conferred directly upon him.[65] That rule does not remove the personal liability of the policeman or other public officer and is, in any case, a principle that has to do with civil rather than criminal liability.[66] The discretionary freedom which R.C.M.P. members may have in performing certain police or national security functions does not, therefore, detract from their personal responsibility for their conduct.

63. It is sometimes said, however, that a peace officer exercising an independent discretion is not to be considered as anyone's servant when he exercises that discretion.[67] That statement is usually relevant in the context of determining whether the Crown or some public authority is vicariously liable for the conduct of the peace officer, or whether his exercise of discretion as to whether

---

[63] See also section 25(o) of the R.C.M.P. Act which makes it a disciplinary offence for a member of the R.C.M.P. to conduct himself in an immoral manner, which may be taken to include acting in breach of the law. Reference may also be made to section 15(1), which requires every member of the Force to take an oath of office in which he swears that he "will well and truly obey and perform all lawful orders and instructions that I receive".

[64] *R.* v. *C.B.C.* (1980) 16 C.R. (3d) 78 (Ont. C.A.).

[65] See *Schulze* v. *The Queen* (1974) 47 D.L.R. (3d) (F.C.T.D.) and the cases referred to therein.

[66] See P.W. Hogg, *Liability of the Crown, in Australia, New Zealand and the United Kingdom*, Melbourne, Law Book Co., 1971, at pp. 104-8.

[67] *Ibid.*, at p. 212.

to arrest or to prosecute is subject to control. We do not think that the principle is one of general application to all the functions of a peace officer.

64. Even if members of the R.C.M.P. are not servants or agents of the Crown, Crown immunity might be applicable. There are instances in which persons other than Crown servants or agents have received the benefit of immunity, the important question in every case being whether the Crown would be prejudiced by subjecting that person to the burdens of the statute. Therefore, immunity is potentially available even if a peace officer who is a member of the R.C.M.P. does not act as a Crown servant in performing a particular function. The criterion for determining whether the rule of immunity from statute is available remains whether there might be prejudice to the Crown, or interference with Crown business (as it is sometimes put), in subjecting the peace officer to criminal liability.

65. Finally we turn to the suggestion made by counsel for the R.C.M.P. that members of the R.C.M.P. "performing national security functions" may be immune from prosecution for "reasonably necessary acts committed in the course of their duties". We think that this proposition is insupportable. It amounts to a defence of "Act of State" or "State necessity", but that defence is not recognized by our law. In the great case of *Entick* v. *Carrington*, the Chief Justice, Lord Camden, said:

> With respect to the argument of State necessity, or a distinction that has been aimed at between state offences and others, the common law does not understand that kind of reasoning, nor do our books take note of any such distinctions.[68]

As was said by an Australian judge,

> It is not the English view of law that whatever is officially done is law — a view adopted by some jurists on the Continent of Europe — on the contrary, the principle of English law is that what is done officially must be done in accordance with law.[69]

A writer on constitutional law has said:

> The Continental constitution often recognizes a "police power", under which the government may act in a general way for the preservation of the public peace or safety. No such doctrines are recognised by the common law of England. With us a public authority must point, if questioned, to some specific rule of law authorising the act which is called in question.[70]

We believe that Canadian law conforms to the above statements.

66. On several occasions we have seen references in R.C.M.P. files to the general proposition that government officials, who are responsible for national security, must be the sole judges of what national security requires. This is the old doctrine of state necessity, which is obsolete. R.C.M.P. memoranda cite, as

---

[68] (1765) 19 State Tr. 1065.

[69] *Arthur Yates & Co. Pty., Ltd.* v. *The Vegetable Seeds Committee* (1945) 72 C.L.R. 37 at 66, per Sir John Latham, C.J.

[70] R.F.V. Heuston, *Essays in Constitutional Law*, 2nd ed., London, Stevens & Sons, 1964, at p. 34.

modern authority for that view, the following words from a 1977 English case, *R.* v. *Secretary of State for the Home Department, ex parte Hosenball*:[71]

> But this is no ordinary case. It is a case in which national security is involved, and our history shows that, when the state itself is endangered, our cherished freedoms may have to take second place.

However, it is misleading to quote this statement out of context. The case concerned an alien whom the Home Office ordered to be deported in the interests of national security because the Secretary of State had information that the alien had obtained information for publication harmful to the security of the nation, including information prejudicial to the safety of servants of the Crown. The alien claimed that he was entitled to see the report which was made about him by a non-statutory advisory Committee which reported to the Secretary of State before the deportation order was made. He contended that natural justice so entitled him. It was in answer to that contention that the above statement was made by Lord Denning, who then continued:

> Even natural justice itself may suffer a set-back... In the first world war, in *R.* v. *Halliday*,[72] Lord Finlay L.C. said: 'The danger of espionage and of damage by secret agents... had to be guarded against.'... But times of peace hold their dangers too. Spies, subverters and saboteurs may be mingling amongst us, putting on a most innocent exterior...
>
> If they are British subjects, we must deal with them here. If they are foreigners, they can be deported. The rules of natural justice have to be modified in regard to foreigners here who prove themselves unwelcome and ought to be deported.

It is thus quite inappropriate to quote what Lord Denning said outside the context of whether the principles of natural justice apply to the exercise of a power to deport, as if it were authority for altering the norms that bind the policeman when national security is involved.

(b) *Intergovernmental immunity*

67. It is probably not within the constitutional powers of the provincial legislatures to impose liability on the Crown in the right of Canada. In the leading case, *Gauthier* v. *The King*, the Supreme Court of Canada held that provincial legislation cannot *proprio vigore* take away or abridge any privilege of the Crown in right of the Dominion.[73]

---

[71] [1977] 3 All E.R. 452 at 457.

[72] [1917] A.C. 260 at 270.

[73] (1918) 56 S.C.R. 176 at 194. It may be difficult to reconcile this decision with the later decision of the Privy Council in *Dominion Building Corporation* v. *The King* [1933] A.C. 533. See D. Gibson, "Interjurisdictional Immunity in Canadian Federalism" (1969) 47 *Can. Bar Rev.*, 40 at 51. However, it has been argued that the two cases can be reconciled: McNairn, *Government and Intergovernmental Immunity in Australia and Canada*, p. 98. Moreover, there have been several *dicta* in the Supreme Court of Canada supporting the *Gauthier* decision: *The King* v. *Richardson* [1948] S.C.R. 57, *The Queen* v. *Breton* (1968) 65 D.L.R. (2d) 76 (S.C.R.).

It may be that this immunity is more extensive than the immunity called "Crown immunity", which, as has already been noted, is also available to the federal Crown when faced with the imposition against it of a provincial statute. The immunity now being considered is one rooted not in the Crown prerogative applicable to both unitary and federal states, but in the constitutional order peculiar to a federal state. This "intergovernmental immunity" may go as far as to protect the federal Crown from provincial statutes even when they, by their express terms, are said to apply to the federal Crown. In that case, of course, "Crown immunity" would not be available because of the specific reference to the federal Crown in the provincial legislation. While "intergovernmental immunity" *may* have this broader effect, it is not *clear* that it does.[74]

68. If "intergovernmental immunity" does have this larger role, a member of the R.C.M.P. would be able to assert immunity, in a proper case, from prosecution for a provincial offence even though the provincial statute creating that offence expressly purported to bind the federal Crown.

69. If a member of the Force should choose to rely on Crown immunity or intergovernmental immunity, it is likely that he would have to show some particular prejudice to federal Crown interests if the provincial statute in question were to apply to him. The threshold test of interference with Crown functions relates logically to both forms of immunity.

(c) *"Exclusive power" or "interjurisdictional" immunity: the general immunity of federally controlled operations from provincial laws*

70. Operations and enterprises which fall under the legislative jurisdiction of the Parliament of Canada must generally abide by the laws of the provinces within which they carry on operations.[75]

71. On the other hand, enterprises which are under federal jurisdiction with respect to their primary operational aspects are immune from provincial statutes which go to the heart of their operations. Such provincial legislation does not apply because the jurisdiction of the Parliament of Canada is exclusive in relation to all those matters which are "an integral part of its primary competence" over such enterprises.[76]

72. When it is held that provincial legislation does not apply to an area which is within the constitutional authority of the federal Parliament, there is sometimes said to be an "exclusive power immunity" or an "interjurisdictional immunity" from the provincial legislation.

---

[74] See McNairn, *Governmental and Intergovernmental Immunity in Australia and Canada*, at pp. 33-40. McNairn's analysis is commented on by Gibson, (1978) 4 *U.T.L.J.* 445.

[75] e.g. *C.P.R.* v. *Notre-Dame de Bonsecours* [1899] A.C. 367.

[76] *Construction Montcalm Inc.* v. *Minimum Wage Commission* [1979] 1 S.C.R. 754, at 768-9 (Mr. Justice Beetz).

73. The federal Parliament has the constitutional authority to establish and provide for the management of the R.C.M.P.[77] The primary basis for this authority would appear to be the peace, order and good government clause of section 91 of the British North America Act.

74. The key question, therefore, is whether control of the conduct of R.C.M.P. officers, acting in the course of their duties, should be taken to be "an integral part of primary federal competence" over the Force. The answer to that question will depend upon the circumstances. The problems dealt with by certain provincial laws would in many situations not form "an integral part" of federal jurisdiction over the R.C.M.P. For example, a municipal by-law relating to garbage disposal and imposing a penalty for violation of its requirements would certainly apply to R.C.M.P. members responsible for operating a staff cafeteria. On the other hand, a member of the R.C.M.P. will have an immunity from provincial legislation based on this ground, if the application of that legislation to him would amount to an encroachment on Parliament's jurisdiction to deal with the management and supervision of the Force. For example, a provincial statute which provides rules of conduct for all peace officers and sets up disciplinary procedures to ensure compliance with them would not be applicable, on this basis, to peace officers in the service of the R.C.M.P.[78] Another example would be a municipal anti-noise by-law, which would not apply to the use of cruiser-car sirens by R.C.M.P. officers in the course of their duties, even if the by-law did not have a built-in exception for emergency vehicles.

75. Generally speaking, the application of provincial penal statutes to members of the R.C.M.P. would not appear to be inconsistent with maintaining the integrity of Parliament's power to provide for the management and administration of the force.[79] Disciplinary measures internal to the R.C.M.P. could still be taken with respect to conduct that constituted a provincial offence, subject to any applicable rules designed to prevent double jeopardy. To the extent that Parliament might see provincial laws as an embarrassment to the R.C.M.P. and their invocation against a member of the Force to be intolerable, it could effectively oust the provincial laws by providing specifically that they were not to apply to members of the R.C.M.P.[80] (The doctrine of paramountcy, discussed in (d) below, would apply.) There is in fact no federal legislation which currently does that. In the absence of such legislation, members of the

---

[77] See *Attorney General of the Province of Quebec and Keable* v. *Attorney General of Canada et al.*, [1979] 1 S.C.R. 218, and *The Attorney General of Alberta and the Law Enforcement Appeal Board* v. *Constable K.W. Putnam and Constable M.G.C. Cramer and the Attorney General of Canada*, [1980] 22 A.R. 510, [1980] 5 W.W.R. 83 [affirmed on appeal to the Supreme Court of Canada on May 28, 1981].

[78] See *The Attorney General of Alberta and the Law Enforcement Appeal Board v. Constable K.W. Putnam and Constable M.G.C. Cramer and the Attorney General of Canada*, [1980] 22 A.R. 510, [1980] 5 W.W.R. 83. This was a decision of the Court of Queen's Bench of Alberta. The Alberta Court of Appeal upheld the decision, but apparently on the ground of paramountcy, rather than on the ground of exclusive power immunity.

[79] But see *R.* v. *Anderson* [1930] 2 W.W.R. 595.

[80] See *R.* v. *Sanford* [1939] 1 D.L.R. 374 (N.S.S.C. in banco).

R.C.M.P. would, except to the extent of the availability of the immunities already discussed, be subject to provincial statutes creating offences, just as the operator of a bus service which constitutes an interprovincial undertaking, who is subject to exclusive federal jurisdiction for regulatory purposes, is nonetheless bound to comply with provincial highway traffic laws.[81]

76. We note that counsel for the R.C.M.P. has urged that this form of immunity has a much broader scope than we think is likely acceptable in law. He suggests that the immunity goes so far as to provide immunity from provincial legislation in relation to matters which, on their federal aspect, are simply "necessarily incidental" to the regulation of the R.C.M.P. In our opinion, the immunity that covers matters that are an "integral part" of the federal competence is not available when the matters are simply "necessarily incidental" to the regulation of the R.C.M.P. It is only with respect to matters which are "integral" to R.C.M.P. operations that provincial laws may be contravened with impunity. The words 'integral' and 'incidental' are virtual opposites.

77. Even if this "exclusive power" immunity might otherwise exist in favour of members of the R.C.M.P. (which we do not agree is so as a universal proposition), such an immunity may be eliminated by Parliament.[82] Presumably it may also be eliminated by delegated legislation enacted by authority of an Act of Parliament. If so, it becomes relevant to refer to section 25 of the R.C.M.P. Regulations:

> It is the duty and responsibility of every officer and of every person in charge of a post to ensure that there is at all times *strict observance of the law*, compliance with the rules of discipline and the proper discharge of duties by all members of the Force.
>
> (our emphasis is added.)

This may be strong evidence of an intention on the part of the Governor in Council that not only federal but provincial laws be observed. There is nothing in the surrounding language of the Regulations or in the R.C.M.P. Act itself to indicate an intention that officers should comply with only some of the laws in the provinces where they function. In the absence of such indication, it is probable that the expression "strict observance of the law" should be given its normal full meaning. If so, such "exclusive jurisdiction" or "interjurisdictional" immunity as might otherwise be available to R.C.M.P. personnel has been eliminated.

78. Counsel for the R.C.M.P. also seems to suggest that "interjurisdictional" immunity would apply even to R.C.M.P. members performing the functions of a provincial police force in those provinces that have contracted with the

---

[81] See *Attorney General of Ontario* v. *Winner* [1954] A.C. 541, at 579 (P.C.). See also *R.* v. *Pearsall* (1977) 80 D.L.R. (3rd) 285 (Sask. C.A.), in which a provincial prohibition against using an aircraft for the purpose of hunting game was held to be valid notwithstanding that aeronautics is subject to federal jurisdiction under the peace, order and good government power of section 91 of the B.N.A. Act.

[82] See D. Gibson, "Interjurisdictional Immunity in Canadian Federalism" (1969) 47 *Can. Bar Rev.* 40, at 46 ff.

federal government for such services. Such arrangements are entered into by the Solicitor General under section 20(1) of the R.C.M.P. Act, which reads in part as follows:

> 20. (1) The Minister may, with the approval of the Governor in Council, enter into arrangements with the government of any province or, with the approval of the lieutenant governor in council of any province, with any municipality in the province, for the use or employment of the force, or any portion thereof, in aiding the administration of justice in the province or municipality, and in carrying into effect the laws in force therein;

We find it very difficult to see how the activities of the R.C.M.P., which are carried out pursuant to a contract relating to internal provincial policing, could be said to be "integral" to Parliament's "primary" jurisdiction over the R.C.M.P. Section 20 limits the purpose of all such contractual arrangements to "aiding the administration of justice in the province or municipality, and- . . . carrying into effect the laws in force therein". "Administration of Justice in the Province" is, of course, a specific head of provincial jurisdiction under section 92 of the B.N.A. Act. Since interjurisdictional immunity exists for the purpose of protecting the exercise of *federal* constitutional jurisdiction from provincial restrictions, it would make no sense to apply the immunity to individuals who are performing functions within the constitutional competence of the provinces.

79. Our conclusion in this regard is in no way affected by the provisions of the current form of agreement with eight of the provinces, which provides that the "internal management" of the Force while engaged in provincial policing shall remain under federal control. In our opinion the words "internal management" cannot be construed to include liability of members of the Force for breaches of provincial law. Moreover, paragraph 4 of the agreement makes it abundantly clear that the Force is generally responsible to the provincial attorneys general with respect to provincial policing:

> 4. (1) The Commanding Officer of the Provincial Police Services shall for the purposes of this agreement act under the direction of the Attorney-General in the administration of justice in the Province.
>
> (2) Nothing in this agreement shall be interpreted as limiting in any way the powers of the Attorney-General, relating to the administration of justice within the province.

In any event, whatever the provisions of the agreement, we think that such an agreement cannot alter the duty owed in law by a member of the R.C.M.P. in regard to conduct that is an offence under the provincial statute. For all these reasons, therefore, we conclude that whatever limited interjurisdictional immunity *may* be available to members of the R.C.M.P. (and we think there is no such immunity generally available except, for example, in regard to disciplinary powers), it does not extend to members performing functions under federal-provincial contracts.

(d) *Immunity as a result of the paramountcy of federal legislation*

80. It is a commonplace of Canadian constitutional law that if an otherwise valid provincial statutory provision and a competent federal statutory provision

cover the same ground and the application of each to a particular set of facts gives rise to a conflict, the federal enactment will be paramount.[83] The provincial provision will be displaced, at least in its application to that fact situation.

81. It is undeniable that the Parliament of Canada has the constitutional jurisdiction to make laws about the R.C.M.P.[84] So, according to counsel for the R.C.M.P., if the R.C.M.P. Act conflicts with provincial law, the paramountcy of the R.C.M.P. Act might be a basis for a claim of immunity from the provincial law by R.C.M.P. members. Counsel for the R.C.M.P. argues that a conflict, and therefore federal paramountcy, arises from the fact that "the area of discipline, management and control of members of the R.C.M.P. performing reasonably necessary acts in the course of duty is fully occupied by" Part II of the R.C.M.P. Act and the R.C.M.P. Regulations. The flaw in this argument is that Part II and the Regulations involve only such matters as insubordination, immorality and ineptitude, and do not include *illegal* acts. In other words, the disciplinary offences under the Act are by no means co-extensive with the offences generally provided by provincial laws. The disciplinary offences are, in many ways, much more extensive, reaching immoral conduct generally, and not just specifically proscribed acts. Far from being "fully occupied", the field of trial and punishment of R.C.M.P. personnel for breaches of the law — federal or provincial — is left entirely untouched by the R.C.M.P. Act. Indeed, in two respects the Act and the Regulations may be said to have an effect which is the opposite of "occupying the field". First, as far as civil liability is concerned, section 37(3) of the R.C.M.P. Act acknowledges that provincial laws will continue to operate with respect to R.C.M.P. personnel. It reads:

> Nothing in subsection (2) prejudices any right or remedy that may exist apart from this section against any person, including the Crown, for any injury to the person or damage to or loss of property in respect of which a member is under this section ordered to make payment of damages or restitution...

Second, section 25 of the Regulations, which has already been quoted, expressly requires every officer and every person in charge of a post "to ensure that there is at all times strict observance of the law". Apart from such specific points, the Canadian courts have adopted a very strict or narrow test of conflict for this purpose, with the result that there is considerable room for the concurrent operation of federal and provincial legislation.[85]

82. For all these reasons our conclusion is that there is nothing in the R.C.M.P. Act or Regulations which suggests that there was an intention to displace any provincial laws in their application to members of the Force. It

---

[83] See, for example, *Attorney General of Ontario* v. *Attorney General of Canada* [1896] A.C. 348 at 366 (P.C.).

[84] *Attorney General of Quebec and Keable* v. *Attorney General of Canada et al.* (1978) 90 D.L.R. (3d) 161 at 180, (S.C.C.) per Mr. Justice Pigeon.

[85] See P.W. Hogg, *Constitutional Law of Canada*, Toronto, Carswell, 1977, at pp. 101-110.

follows that there is no basis for a claim of immunity based upon the paramountcy doctrine.

F. AUTHORIZATION BY MINISTERS

83. If a member of the R.C.M.P. were charged with an offence, arising out of his selfless conduct intended to protect the security of Canada or the public good and not to advance his own interests, would he be entitled to raise as a defence that the Solicitor General or the federal Cabinet had, expressly or by implication, authorized illegal activities in general or the specific act or activity which gave rise to the charge?

84. Senior members of the R.C.M.P. have a habit of referring to Ministers as their "political masters". Does this mean that such authority might be regarded as a "superior order" (to the extent that there is a defence of superior orders)? The answer must be no in the case of the Cabinet, which is not in law a "superior" to members of the R.C.M.P. unless it speaks by regulation. In the case of the Solicitor General, he might be regarded as a "superior" in view of his power of direction found in section 5 of the R.C.M.P. Act.

85. However, the kind of hypothetical situation which we are considering here is the effect in law not of an "order" but an "authority", that is, some sort of express or implied permission or licence to do that which is unlawful. Does the law recognize that such a licence can relieve a member of the R.C.M.P. from liability for a statutory offence or a civil wrong such as trespass? The answer is no. To allow such a defence would violate a fundamental constitutional principle, established in the Bill of Rights in 1689 and the cases interpreting its prohibition of the prerogative of dispensing and suspending laws.

> In the Bill of Rights it was declared
>
> 1. That the pretended power of suspending of laws, by regal authority, without consent of parliament, is illegal.
>
> 2. That the pretended power of dispensing with laws, or the execution of laws, by regal authority, as it hath been assumed and exercised of late, is illegal.[86]

As far as the dispensing power was concerned, the foregoing spoke only of the past. However, the dispensing power was prohibited for the future as well:

> ...[N]o dispensation by non obstante of or to any statute or any part thereof, shall be allowed, but... the same shall be held void and of no effect, except a dispensation be allowed of in such statute...

Thus the present rule of constitutional law is stated as follows by Halsbury's *Laws of England*:

> The Crown may not suspend laws or the execution of laws without the consent of Parliament; nor may it dispense with laws, or the execution of

[86] 1 Will. & Mar. sess. 2 c.2. *Halsbury's Statutes of England*, 3 ed., vol. 6, p. 489. Also found in C. Stephenson and F.G. Marcham, *Sources of English Constitutional History* (Rev. ed.), New York, Harper and Row, 1972.

laws; and dispensations by *non obstante* of or to any statute or part thereof are void and of no effect except in such cases as are allowed by statute.[87]

The suspending and dispensing powers which had been used before the Glorious Revolution of 1688 were explained in a Canadian case, in which Chief Justice Freedman of Manitoba said:

> The distinction between these two ancient powers may be briefly noted. By virtue of the suspending power the Crown suspended the operation of a duly enacted law of Parliament, and such suspension could be for an indefinite period...
>
> Under the dispensing power the Crown purported to declare that a law enacted by Parliament would be inapplicable to certain named individuals or groups. By virtue of a dispensation in their favour the law would not apply to them, but it would continue to apply to all others. It has been said that the dispensing power "was derived from the Papal practice of issuing bulls *non obstante statuto*, 'any law to the contrary notwithstanding'" . . . [88]

Chief Justice Freedman then quoted the English historian, F.W. Maitland, who in discussing the Bill of Rights, had asserted: "This is the last of the dispensing power". Chief Justice Freedman then continued:

> "This is the last of the dispensing power." Maitland could never have thought that in the year 1968, nearly three centuries after the *Bill of Rights*, a certain departmental official of Manitoba, acting in fact or in law under the authority of his Minister, would purport to grant a dispensation in favour of a certain group, exempting them from obedience to a particular law to which all others continued to remain subject.

Chief Justice Freedman then added:

> The other point is that nothing here stated is intended to curtail or affect the matter of prosecutorial discretion. Not every infraction of the law, as everybody knows, results in the institution of criminal proceedings. A wise discretion may be exercised against the setting in motion of the criminal process. A policeman, confronting a motorist who had been driving slightly in excess of the speed limit, may elect to give him a warning rather than a ticket. An Attorney-General, faced with circumstances indicating only technical guilt of a serious offence but actual guilt of a less serious offence, may decide to prosecute on the latter and not on the former. And the Attorney-General may in his discretion stay proceedings on any pending charge, a right that is given statutory recognition in s.508 [am. 1972, c. 13, s.43(1)] and s.732.1 [enacted idem, s.62] of the Criminal Code. But in all these instances the prosecutorial discretion is exercised in relation to a specific case. It is the particular facts of a given case that call that discretion into play. But that is a far different thing from the granting of a blanket dispensation in favour of a particular group or race. Today the dispensing power may be exercised in favour of Indians. Tomorrow it may be exercised in favour of Protestants, and the next day in favour of Jews.

[87] 4 ed., vol. 8, para. 912.

[88] *Regina* v. *Catagas* (1978) 81 D.L.R. (3d) 396 at 397-8 (Man. C.A.) per Chief Justice Freedman. See also *R.* v. *London County Council* [1931] 2 K.B. 215 at 228; *London Borough of Redbridge* v. *Jacques* [1971] 1 All E.R. 260.

> Our laws cannot be so treated. The Crown may not by Executive action dispense with laws. The matter is as simple as that, and nearly three centuries of legal and constitutional history stand as the foundation for that principle.

86. While the law precludes reliance on executive suspension or dispensation as a defence, the circumstances as a whole, including any such purported suspension or dispensation, may be invoked in mitigation of sentence. No generalization is possible as to the effect such a licence might have on the question of sentence.

CHAPTER 2

EXTENUATING CIRCUMSTANCES

1. In the foregoing chapter we discussed whether there are legal defences open to members of the R.C.M.P. if they were charged with offences or sued arising from their having been engaged in the kinds of investigative practices and other procedures we discussed in Part III, Chapters 2 to 10. Our conclusion was that in most cases the defences raised would likely fail as a matter of law.

2. That does not, however, dispose of the matter fully. Although all the issues discussed in Chapter 1 may not be the basis of defences in law to charges or suits, the same circumstances might properly be factors to be taken into account — not as a matter of right but of grace — when the decision is being taken whether or not to prosecute, what the appropriate sentence is, and whether a pardon should be granted. When these decisions are being made, at least two additional considerations may be applicable to members in the lower ranks of the police force. These are first, that a member's actions were motivated by noble objectives — enforcing the law or preserving national security — and second, that he received ambiguous policy instructions from senior management as to whether or not it was appropriate at times to commit an unlawful act or to refuse to obey an unlawful order. We cannot imagine any member of a lower rank successfully raising either of these considerations as a legal defence. Yet he might ask that these matters be taken into account when discretion is being exercised in making the three kinds of decisions referred to. We examine each of these considerations below.

The pursuit of law enforcement or national security objectives

3. A member of the R.C.M.P. might argue, in seeking a favourable exercise of prosecutorial discretion, or in mitigation of sentence or in applying for a pardon, or in seeking at least public sympathy, that what he had done was in pursuit of law enforcement or national security objectives as he understood them to be defined and approved by the senior management of the Security Service or the R.C.M.P., or by the "political masters". Thus, it would be argued, he was motivated by noble purposes and not self-interest. This is a question with which we shall deal in a subsequent Report when we consider specific factual situations. All we wish to say here is that, while mercy and compassion are among the important considerations to be taken into account in assessing such an argument, it is also important not to encourage a belief by members of a police force or a security intelligence agency that if they break the law they will be protected by "the system", even if not by the law. We note that this justification of noble purpose — justification which in this context

may affect the treatment which might be afforded the member consequent upon a breach of the law — is distinct from the defence based on lack of "evil intent". We examined and rejected this defence in Chapter 1 of this Part. Nevertheless, common to both the 'defence' and the 'extenuating circumstances' arguments is the motivation of the member. The point at which and purpose for which each of these arguments is advanced often become blurred, thus leading to considerable confusion.

Ambiguous policies adopted by senior management

4. It is also important that members of the police force or security intelligence agency who are at the level of senior management should not think that members should consider it as a duty to obey policies adopted (formally or informally) by senior management, that tolerate violations of the law. On the other hand, members are entitled to expect senior management to give them clear instructions as to what conduct is permissible and within the law, and what conduct is unacceptable and unlawful. Senior management has a duty to ascertain what the law is in order that the law may be obeyed by the members. An opinion of the Judicial Committee of the Privy Council has stated that

> It is the duty of the Crown and of every branch of the Executive to abide by and obey the law. If there is any difficulty in ascertaining it the Courts are open to the Crown to sue, and it is the duty of the Executive in cases of doubt to ascertain the law, in order to obey it, not to disregard it.[1]

Moreover,

> ... matters of practice and policy of the Government and of any department thereof are not to be permitted to override the performance of the duty [quoted above].[2]

5. It will not always be possible or desirable for the instructions to be applied mechanically. Some doctrines of the law that give a defence to a criminal charge or a civil suit must be stated in broad terms, such as the doctrine of necessity, which we discussed in Chapter 1 of this Part. No answers can be provided in advance as to how to react lawfully in the case of emergencies such as are contemplated by that defence: no one can expect senior management to do more than state guidelines that are in accordance with the law.

6. However, more can be expected in the direction of operations that do not involve emergencies. Instructions can be more precise. The member engaged in an operation is entitled to expect direction based upon carefully conceived policies that comply with the law.

7. Members are entitled to receive more assistance than Commissioner Higgitt thought sufficient in 1970. In June 1970, some members of the Security Service, in a training class, questioned their position if criminal or civil action were to be brought against them. Their concern referred to carrying out what were described, in a memorandum (Ex. M-1, Tab 2) summarizing the

---

[1] *Eastern Trust Co.* v. *McKenzie, Mann & Co.* [1915] A.C. 750, 22 D.L.R. 410 (Privy Council).

[2] *Glazer* v. *Union Contractors Ltd.* (1960) 25 D.L.R. (2d) 653.

discussion, as "certain tasks performed by S.I.B. [Security and Intelligence Directorate] or C.I.B. personnel" that required "that the law be transgressed, whether it be Federal, Provincial or Municipal law, in order that the purpose of the undertaking may be fulfilled". The memorandum observed that "The particular task will have been sanctioned in many cases by a number of officers who will at least be aware of the means required to achieve the end product, and who will have given their tacit or express approval".

8. The members of the class wanted to know to what extent the Force would back its members in these circumstances, whether their families would be cared for in the event of imprisonment and where members stood in terms of future employment. The Legal Branch suggested that members be told that if there were express approval of a particular operation by a superior, or a superior were aware of "the means required to achieve the end results" and had given implied approval by communicating the fact of his knowledge to the member, an attempt should be made to persuade the Attorney General to stay any criminal proceedings; if conviction should result, the Commissioner should retain the member in the Force; the Force should pay any fine; and, in the event of imprisonment, the member's employment should be continued. The Legal Branch also suggested that if a member acted independently without authority, and if he were convicted the Commissioner could, both morally and legally, discharge the member as he was acting outside the scope of his employment. In both situations the Legal Branch also suggested when counsel should be provided, but that need not be summarized here (Ex. M-1, Tab 3).

9. The Deputy Commissioner (Criminal Operations), J.R. Carrière, expressed approval of these views, which he felt could not be published in policy instructions but could be made available to Commanding Officers and C.I.B. officers so that they could advise members. He also felt that these views could be imparted to members attending certain training courses and seminars. In addition, the Director General, Security and Intelligence, Mr. Starnes, agreed with the views expressed by the Legal Branch and made similar suggestions as to how they might be transmitted to members engaged in Security and Intelligence work.

10. A three-page policy memorandum was then prepared for Commissioner Higgitt's approval. This memorandum, in addition to incorporating the points noted above, contained the following paragraph which is ambiguous and may even contradict itself:

> It must also be borne in mind, of course, that where a member is directed to perform a duty which may require him to contravene the law for any purpose or where the means required to achieve a specific end can reasonably be foreseen as illegal, a member is within his rights to refuse to do any unlawful act. Such a refusal may be given with *impunity*. Though no disciplinary action would be taken, *a transfer may be indicated in such a situation* (Ex. M-1, Tab 7).
>
> (The emphasis is ours.)

11. Commissioner Higgitt refused to sign this policy memorandum. Instead he decided, and noted on the memorandum that

> Under no circumstances should anything of this nature be circulated in written or memo form. The reasons ought to be obvious. I do not believe this is the problem it is being made out to be. Members know or *ought* to that whatever misadventure happens to them the Force will stand by them so long as there is *some* justification for doing so.
>
> (Ex. M-1, Tab 7.)

In view of this decision, the Deputy Commissioner (Administration) instructed the Director of Organization and Personnel to put the communications concerning this matter away "in secret envelope on policy file", and that the contents were "to be relayed to S. & I. and C.I.B. classes orally when convene [sic] at H.Q. Ottawa". The draft policy memorandum was conveyed to an officer for the information of lecturers and to Mr. Starnes.

12. In his testimony concerning this policy matter, Mr. Higgitt made several noteworthy points. First, he confirmed the validity of the problem which gave rise to efforts within the R.C.M.P. to develop the policy memorandum referred to above:

> The problem at the moment was members of the Force... getting themselves into difficult situations as a result of quite straight forward, honest carrying out of their duties, getting themselves into difficulties, it could be with transgressions of a law or it could be with a number of other things; it was a problem that was inherent in not only the Security Service, in the law enforcement generally, that occasionally placed members in difficult circumstances. (Vol. 88, p. 14452; see also Vol. 85, pp. 13965-6 and Vol. 87, pp. 14330-1.)

13. Second, it is not clear from his testimony what Mr. Higgitt believed the R.C.M.P. policy to be for dealing with this problem. At several points, Mr. Higgitt stated that the draft policy memorandum was, in effect, Force policy:

> Q. So, the text of the draft letter did remain the policy as it is explained there, as it is expressed there?
>
> A. Right, in essence it was the policy. (Vol. 85, p. 13948; see also Vol. 84, p. 13751.)

Nonetheless, at other points, he testified that the draft memorandum did not represent Force policy. Rather, he said that his handwritten note quoted above was the extent of Force policy (Vol. 87, pp. 14282, 14289, 14303). Notwithstanding this lack of clarity about what precisely was Force policy, Mr. Higgitt testified that this policy had been in effect for over 30 years and that his handwritten note was not intended to change the policy in any way. Rather, it was "restating the obvious" (Vol. 85, p. 13992 and Vol. 86, p. 14190). Furthermore, he gave three reasons why the policy on this matter should not have been written down and circulated among R.C.M.P. members:

(a) the policy was well known to members (Vol. 84, p. 13751 and Vol. 86, pp. 14190-1);

(b) the problem addressed by the policy was not as significant as it was being made out to be and publication of the policy might have the effect of

". . . giving some degree of freedom which, certainly, I did not wish to give in that way to members at large to engage in this sort of thing" (Vol. 84, pp. 13751-2); and

(c) Mr. Higgitt believed that there was ". . . really no answer that one can put in written form to the problem involved here. . . you could not begin to describe the various things that could happen. You can't describe, except in a very general way, what the Commissioner's response would be to those things" (Vol. 87, pp. 14282-3). Notwithstanding these reasons for not writing down the policy, Mr. Higgitt believed that the policy should have been communicated orally to those members of the Force likely to be affected (Vol. 85, p. 13940).

14. Third, contrary to the draft policy memorandum, Mr. Higgitt testified that the Force would not necessarily stand behind the member who obeyed an unlawful order given by a superior:

> Q. Would I be correct then that in a situation, say, where a senior N.C.O. instructed a constable to do something that involved a transgression of the law, that under your policy, that the constable would be protected by the policy, but the N.C.O. would not be?
>
> A. That is a question that could only be answered given the circumstances. Protection wasn't necessarily always involved. (Vol. 85, pp. 13992-3.)

On the other hand, Mr. Higgitt stated that if a member disobeyed an unlawful order, he might well be transferred, although in Mr. Higgitt's view, such a transfer would not be "a disciplinary matter" (Vol. 85, pp. 13959-64).

15. Members of a police force or a security intelligence agency at the operational level are entitled to receive guidance as to the law so that they may obey the law, not disregard it. Because the members of any agency of the State must abide by and obey the law, they are entitled to receive advice that is as precise as possible so that they may remain within the law. While support for members who are charged with offences is acceptable, the rationale of the support must not be expressed in such a way as to suggest that express or tacit approval by a superior will relieve members in all circumstances of the obligation to obey the law. Based on our review of this episode, we conclude that a member of the R.C.M.P. during this period could argue with considerable justification that he did not receive the advice and guidance he was entitled to. Rather, it would be surprising if he did not find Force policy on this matter vague, confusing and at times contradictory. Moreover, he would have grounds for concluding that (a) there were times when the Force would expect him to disobey the law, and (b) he might be punished if he refused to obey an unlawful order.

16. In conclusion, while the blame to be attached to "foot soldiers" for breaking the law cannot be absolved by the failure of management to provide clear and proper instructions, the consequences which flow from such law breaking may be affected by that failure. It is a factor that, depending on all the circumstances, may properly be taken into account in the exercise of prosecutorial discretion, the determination of the appropriate sentence, or the decision whether to grant a pardon.

PART V

A PLAN FOR THE FUTURE: ROLE, FUNCTIONS AND METHODS OF A SECURITY INTELLIGENCE AGENCY

INTRODUCTION

CHAPTER 1: Fundamental Principles

CHAPTER 2: A Security Intelligence Plan for the Future: A Summary

CHAPTER 3: The Scope of Security Intelligence

CHAPTER 4: Information Collection Methods

CHAPTER 5: Analysis, Reporting, and Advising Functions

CHAPTER 6: Executive Powers and Preventive Activities

CHAPTER 7: International Dimensions

CHAPTER 8: Relationships with other Departments, Provincial and Municipal Authorities

INTRODUCTION

1. We now turn from the past to address the future. In Parts V to IX we present an outline for the future of security intelligence work in Canada and make recommendations for statutory and administrative reform. These reforms encompass: the functions of the security intelligence agency; the investigative and other techniques which it should be permitted and enabled by law to employ; the structure of the agency; its relationship with its Minister and the federal government generally; its relationship with Parliament; its relationship with provincial governments and the agencies of foreign countries; the means by which it should be held accountable to ensure effectiveness and to prevent abuses of its powers either by the agency itself or by the federal government; and, changes in existing laws relating to national security.

2. We stress that the recommendations contained in these Parts are put forward as a set of interlocking proposals, of countervailing forces. To accept the recommendation as to the kinds of activities about which the agency should be empowered to collect intelligence, without implementing the recommendations as to scrutiny and control by the Minister, Parliament, and the independent review body would be dangerous. To accept the recommendations about relationships between the agency and the agencies of foreign countries without the same régime of scrutiny or oversight would be dangerous. To accept the recommendations as to the qualities of the men and women who should carry out the agency's tasks without accepting our conviction that those qualities cannot be achieved if the agency remains within the R.C.M.P. would be an exercise in futility. To accept our recommendations as to the ultimate responsibility of the federal government in matters of security intelligence without adopting our views as to the role of the provinces would bedevil the effectiveness of the agency. To expect the agency to carry out the mandate which is imposed upon it by statute without giving it the statutory powers of intelligence collection that are necessary for its effectiveness would be to invite disaster in the face of crisis. To grant the agency powers of intelligence collection which are not possessed by the ordinary citizen without imposing the recommended system of ministerial approval, judicial authorization and *ex post facto* scrutiny by the independent review body and Parliamentary Committee would open the way to unacceptable levels of intrusion into the private lives of our people and perhaps a repetition of the institutional acceptance of disregard of the law.

CHAPTER 1

FUNDAMENTAL PRINCIPLES

1. In Part II of this Report we stated that we have been guided by the fundamental precept that Canada must have effective security within a democratic framework. We must return to that theme here, for it provides the bedrock of principle on which our recommendations for a new security system are based. The changes in structures, procedures and laws that we will recommend should be judged in terms of how well they serve this basic objective. Although in Part II we have already set out our understanding of the requirements of security and the requirements of democracy, we must return to them and relate them more specifically to the role of the Security Service.

2. When we speak of the need for security we have in mind the need for protection against the clandestine activities of agents of foreign powers in Canada and the activities of individuals or groups which threaten the fundamental rights, structures and processes of our democratic system. We believe that it is a responsibility of government in Canada to protect Canadians against these kinds of activities.

3. The protection needed goes beyond apprehending and punishing those who are in the process of committing a crime. There are many contexts, other than law enforcement, in which government needs accurate advance intelligence about persons or groups who may threaten the security of Canada. Foreign powers should not be able to establish networks of espionage and secret interference in this country. If security against attempts to establish such networks is not provided, Canadians' enjoyment of self-government on their own territory is in jeopardy, as is the trust of our allies. Similarly, we think Canadians are unwilling to risk the danger to the exercise of their democratic rights and liberties that would result if the responsible government agencies remained ignorant of the plans and preparations of terrorist or subversive organizations until they surfaced in the form of outright criminal acts. In the next chapter we shall expand on this theme, as it is essential to understanding the need for a security intelligence agency.

4. Thus, the effectiveness of the R.C.M.P. in enabling government to identify and prevent activities threatening the security of Canada is one standard by which we must assess the policies, procedures and laws governing it in the discharge of its responsibility.

5. Effectiveness must not be the only standard for judging security arrangements. As we stressed in the first chapter of Part II, it is essential that our security system also meet the requirements of democracy. This means that because Canada is a democratic country it must tolerate security risks which a

non-democratic state would not. A totalitarian state need put no limit on the extent to which it spies on its own citizens to ensure its survival. In such a country all dissident opinion is suspect, the enjoyment of privacy is not a protected social value, foreign visitors are not free to travel on their own, secrecy rather than openness is characteristic of government decision-making, and the subjection of government officials to the sanctions of the law is not a hallowed feature of the political tradition. In such countries security arrangements need be judged only in terms of their effectiveness. But in Canada the overriding objective of our security arrangements is the preservation of our democratic system. It follows that our security system must be assessed in terms of both its effectiveness and its conformity with the requirements of democracy.

6. In Part II we identified three essential requirements of democracy: responsible government, the rule of law, and freedom of legitimate political dissent. These, we would emphasize, are *requirements* of democracy. As requirements they are not to be compromised, whittled down, or balanced off to make effective security possible.

7. Responsible government must mean that responsible Ministers can know about all the practices and policies of security agencies and about any of their operations which raise policy or legal issues. The security system must be an open book to responsible Ministers and to the Prime Minister. No pages in that book should be sealed because security officials think they contain information too sensitive for Ministers' or Prime Ministers' eyes or ears. Responsible Ministers cannot be expected to know everything that a security agency does, but they *can* and *must* be expected to know the policies governing the operations of the security agency and to establish procedures for ensuring that operations raising difficult policy issues are brought to their attention.

8. Nor is the rule of law a principle that should be compromised for the sake of national security. Government agencies, including a security service, should not pick and choose which laws they will obey. We do not accept the idea that there are some 'minor', 'regulatory', laws which security agencies should be free to ignore when they stand in the way of security investigations. There may well be a need to change the laws so that exemptions are provided for members of a security agency or police force, but it is not for security agencies, or police forces, or even for the Ministers responsible for these agencies, to decide which laws apply to them and which do not. Under the rule of law in our system of government, the legislators, federal and provincial, determine general rules of law, and disputes about the application of the laws to particular cases are decided ultimately by the judges and juries.

9. We should make it clear that when we insist on the rule of law as an absolute principle we have in mind the absolute prohibition of institutionalized unlawfulness. We realize that in all organizations, public and private, there will be members who from time to time break the law. That will happen in the best managed police forces and security agencies. When it does, the rule of law requires that such incidents be reported to the prosecuting authorities and be subject to the regular procedures for the administration of justice. What is

completely intolerable is to permit police and security forces, as a matter of institutionalized practice, to condone certain legal violations by their members as a necessary means of carrying out the responsibilities of their organizations.

10. If governments and police forces do not strictly apply the rule of law to themselves it will become increasingly difficult for them to persuade private organizations and individuals in our society to respect the law. It is essential that those whose function it is to uphold the law should adhere to it themselves. In the words of Mr. Justice Brandeis of the United States Supreme Court:

> Decency, security and liberty alike demand that government officials shall be subjected to the same rules of conduct that are commands to the citizen. In a government of laws, existence of the government will be imperilled if it fails to observe the law scrupulously. Our Government is the potent, the omnipresent teacher. For good or for ill, it teaches the whole people by its example. Crime is contagious. If the Government becomes a lawbreaker, it breeds contempt for law; it invites every man to become a law unto himself; it invites anarchy. To declare that in the administration of the criminal law the end justifies the means — to declare that the Government may commit crimes in order to secure the conviction of a private criminal — would bring terrible retribution. Against that pernicious doctrine the Court should resolutely set its face.[1]

11. The third requirement — democratic dissent — is perhaps the most difficult to maintain because its observance requires such careful judgment. Still, we believe that the distinction can be made between, on the one hand, those who wish to overthrow our democratic system or use violence or threats of violence to violate our democratic procedures, and on the other hand, those who seek radical change in our social, economic or political arrangements within our democratic system. The difficulty of making this distinction in particular cases is not a reason for abandoning it. On the contrary, the importance to democracy of drawing the line correctly between legitimate dissent and subversion calls for sophisticated judgment and political understanding on the part of those who carry out security operations. It also requires sensitive direction by responsible Ministers and independent review of security operations to ensure that the line is properly drawn and maintained.

12. In addition to the essential features of democracy which we have described there are other liberal democratic values which must be balanced against the requirements of security. One such value is individual privacy. In a liberal society the extent to which the state pries into the private life of the individual, secretly intercepts his private communications or enters without his consent onto his private premises, should be kept to a minimum. Individual privacy may not be an absolute value in our society but it is one facet of the enjoyment of freedom and we are sure that Canadians greatly value it and would qualify it only for very pressing, countervailing reasons. Thus, when we turn to consider the investigative techniques which should be available to a security intelligence agency our concern will go beyond maintaining the rule of

---

[1] *Olmstead* v. *United States*, (1928) 277 U.S. 438.

law. It is fundamental that all investigative techniques not lawfully available to the ordinary citizen be provided for by law. However, in considering whether to recommend any changes in the law to provide additional investigative powers for security or police purposes, the need for more effective security or law enforcement must be balanced against the cost of making additional inroads on individual privacy. Indeed we must consider whether the reduction of privacy inherent in existing police and security service powers is justified in terms of the contribution such powers make to security and effective law enforcement.

13. Another liberal value which must be balanced against the requirements of security consists of certain norms of procedural justice. One of these norms requires that when an individual is threatened with penalties by the state, he should know the case against him and has a chance to refute it. But in security screening cases, for instance, there may well be situations where to disclose to the individual the entire case against him would do grave damage to continuing security investigations and imperil the lives of those who have provided security information. Total adherence to the norms of due process in such cases would make it difficult to maintain a feasible security screening system. Similarly, in situations of grave national emergency it may be necessary to extend the period during which persons may be detained without being brought before a judge or magistrate beyond that which we normally deem compatible with our ideal of due process. Here again a careful balancing of security needs and democratic values is required.

14. In judging the extent to which security arrangements should be permitted to encroach on individual privacy or deviate from the requirements of due process, our principle should be to minimize the extent of encroachment or deviation. If these democratic values are as highly prized by Canadians as we believe, they should be departed from only when there is a strong case for holding that it is essential to do so in order to protect the security of Canada. Such values cannot be inviolable: effective protection against genuine threats to the security of Canada will require secret and intrusive methods of investigation and other departures from democratic values. But the guiding principle should be that these reductions in the enjoyment of liberal democratic values and procedures should be held to the minimum required for the safeguarding of the democratic system itself.

15. One further element of Canada's constitutional system, which must be recognized by Canada's security system, is its federal character. Given the national and international character of threats to the security of Canada, it makes good practical sense for the federal government to play the lead role in obtaining advance information about these threats and in ensuring that this information is reported to governments and police forces having the executive responsibility for dealing with such threats. It makes equally good sense for the provincial and municipal authorities to play the lead role in taking police and prosecutorial measures against threats of political violence at the local level. We think the practical requirements of sound security demand effective cooperation among federal, provincial and municipal authorities in determining the division of labour between them in national security matters.

16. Above all, national security must be a field of intergovernmental cooperation: it must not be permitted to become a field of federal-provincial competition. The security of Canadians would be damaged by rival investigative forces spending as much effort watching one another as watching those who threaten Canadian democracy. National security must be recognized as embracing interests that transcend those of either level of government. The measures adopted to protect the security of Canada must recognize that principle.

17. The principles we have set out above are the standards by which we hope our recommendations will be judged. The security system we recommend constitutes a structural edifice of law, institutional arrangements and administrative practice. In our view, the merit of that edifice should be judged in terms of how well it reconciles the requirements of security with the requirements of democracy within the Canadian federal system of government.

CHAPTER 2

A SECURITY INTELLIGENCE PLAN FOR THE FUTURE: A SUMMARY

A. REASONS FOR HAVING A SPECIAL FEDERAL AGENCY FOR SECURITY INTELLIGENCE

1. In considering the policies, procedures and laws which should govern the R.C.M.P. in the discharge of its responsibility to protect the security of Canada, we are concerned first and foremost with the R.C.M.P. Security Service. It is the Security Service which now fulfills the function of Canada's security intelligence agency. Thus our recommendations for Canada's security arrangements will focus on the future of the Security Service. We will be concerned with its intelligence collection role and powers, its role in providing advice to government, especially with respect to security screening and in crisis situations; its relationship with police forces, other federal departments and provincial and municipal authorities, and with foreign agencies; its personnel, internal management and organizational structure; its direction and control by Ministers, and the review of its activities by Parliament and independent bodies.

2. Before we deal with these various features of the security plan for the future, a preliminary question must be faced. Does Canada need an agency at the federal level with the specialized task of a security intelligence agency? Or could the various tasks involved in collecting, analyzing and reporting information about threats to the security of Canada be left to other existing government departments and agencies and to regular police work at the federal, provincial and municipal levels? This is clearly an essential question, for if there were no need for the federal government to maintain an agency which specializes in security intelligence functions, then our leading recommendation in this part of our Report would be to abolish the R.C.M.P. Security Service and not replace it with any distinct organization devoted to security intelligence responsibilities.

3. The question as to whether there is a need for a federal security intelligence organization is also fundamental in terms of public accountability. We believe that we have reached a point in Canadian history when a security service, if it is to serve Canada effectively, must have a clear public mandate. Whatever the merit in the past of keeping the existence and responsibilities of such an organization secret, that practice has had its day in Canada. If there is

to be a security service, especially one with intrusive investigatory powers, both the government and the public must have a clear understanding of the need for it.

4. The question of the need for a national security intelligence organization has two aspects: first, is there a need for intelligence pertaining to national security? Second, is there a need in Canada for a specialized agency at the federal level to provide that security intelligence?

5. Our answer to the first part of the question, as we indicated in Part II, is in the affirmative: Canada does need security intelligence. But this answer means very little unless we explain what we mean by security intelligence. Security intelligence is essentially advance warning and advice about activities which threaten the internal security of Canada. In our First Report we put forward the view that the term 'security of Canada' (or 'national security') involves at least two concepts: first, the need to preserve the territory of our country from attack; second, the need to protect our democratic process of government from violent subversion. In Part II of this Report we referred in general terms to the activities which we regard as constituting the principal threats to the security of Canada. Such activities fall into three general categories: foreign intelligence activities, terrorism, and domestic subversion. With respect to each of these categories we think it important to indicate in more detail the types of activity about which governments and police forces in Canada should have advance intelligence.

Nature of the threats

6. First, as to foreign intelligence activities, it is evident that all of the major powers and a number of other powers have foreign intelligence agencies with mandates to operate in a clandestine or deceptive manner in foreign countries. As we reported in the historical overview at the beginning of this Report, there is ample evidence that members of many of these agencies have been active in Canada. The intelligence agencies of Communist countries remain the most significant threat of this kind in Canada today. There is every indication that these agencies will continue their efforts in Canada in the foreseeable future. But there are many other countries whose secret intelligence activities pose a threat to Canadian democracy and sovereignty, now and in the future. Several Middle Eastern countries, for example, have developed aggressive foreign intelligence agencies and we have reviewed evidence of their activities in Canada. Furthermore, it would be naïve to believe that our sister democracies and military allies would never in the future attempt to pursue their economic or political interests in Canada through their well-funded and highly professional secret intelligence agencies. In a world of increasingly scarce energy resources and tough economic competition it is essential that Canada have a capacity to detect the efforts of any country to advance its interests in Canada by clandestine means.

7. In many instances the objectives of foreign 'intelligence' agencies embrace much more than collecting intelligence. They include a wide range of efforts to promote their own country's interests in Canada by means that go well beyond

acceptable lobbying and diplomatic representation. Such activities have taken several forms. An example is trying to manipulate the political leadership of an ethnic community in Canada by threatening reprisals against relatives in the country of origin. Another is compromising a politician or government official so that under threat of blackmail he acts as an agent of influence for a foreign country. Yet another is cultivating a friendship within our scientific community which leads by imperceptible steps from obtaining open scientific information to obtaining information that could be used to damage Canada's competitive position in international trade. The protection of our citizens, the trust of our allies and, above all, our capacity for self-government, require that we make an effort in Canada to ensure that the government is well-informed about the operations in Canada of all foreign intelligence agencies. Canada's sovereignty as a nation would, we believe, be seriously undermined if the secret intelligence agencies of the world had reason to believe that they had, as it were, a free ride in Canada and could operate here without any fear of detection.

8. Information about foreign intelligence activities is needed in a number of contexts. There is, of course, the law enforcement context, in which information about a foreign agent's preparations to commit espionage or sabotage or actual acts of espionage or sabotage may be used by law enforcement agencies for prosecutorial purposes. But if Canada's security is effectively protected, situations of this kind should be exceptional. The aim should be to have advance intelligence which will enable the government to take preventive measures. It should be borne in mind that foreign intelligence agents very often operate under cover of diplomatic status and because of such status are normally not prosecuted. Those responsible for Canada's international relations need timely and well-informed advice about the secret intelligence proclivities of foreign diplomats, preferably before they are granted diplomatic visas to enter Canada and certainly after they are granted such visas. Numerous other examples of the need for information about foreign intelligence activities can be cited. It is sometimes necessary to warn Canadians travelling abroad about recruitment techniques employed by foreign intelligence agencies, to advise Canadian businessmen about the interest of foreign intelligence agencies in acquiring Canadian technology for their country, and to inform departments of government about the technological capacity of foreign intelligence agencies to intercept communications and gain access to protected information. All of these contexts are well outside regular law enforcement responsibilities.

9. The second category of activity about which security intelligence is needed concerns those political acts which, while not amounting to full-scale rebellion or revolution, involve the use or threat of violence to influence the political process. The modern term for activity of this kind is terrorism. Although terrorism is by no means a new phenomenon, it has assumed dimensions which pose a serious threat to Canada's internal security. To begin with, there has been a significant increase in the international dimension of terrorism. Modern means of communication and transportation have shrunk the world, politically speaking. For example, a group whose terrorist activity is directed at changing political conditions in the Middle East or Latin America may secure financial backing from an African, European or Caribbean country and stage a terrorist

act at an international event hosted by Canada. Mass media have increased the impact which a very small group of fanatics, through a symbolic act of violence, can hope to make on public opinion and government decision-making. The leverage which terrorists can exert increases with the availability of means of mass destruction, including nuclear and bacteriological devices. Although we do not know whether any terrorist group today has the capability of making a nuclear bomb, we do know that the increase in nuclear facilities and traffic in fissionable material will increase the opportunities for this drastic form of political blackmail in the future.

10. We should stress that it is the political form of terrorism with which security intelligence is primarily concerned. Threats or acts of violence by persons with no political motive, while of great concern to those responsible for the security of life and property in Canadian communities, do not threaten to subvert Canada's democratic process of government or infringe on its national sovereignty. But threats of violence designed to force a municipal, provincial or federal government to change its policies are a serious violation of the Canadian system of democratic government. Similarly, politically motivated attacks on representatives of foreign countries visiting Canada or on the embassies or consulates of foreign countries in Canada reduce Canada's capacity to participate responsibly in the community of nations.

11. Acts of political terrorism, when there is reason to believe they are about to occur or after they occur, are properly the concern of law enforcement agencies. But governments and police forces in Canada should have advance intelligence. Immigration authorities, for example, should have information about international terrorists to be able to identify them when they apply for entry to Canada. When international events such as the Habitat Conference, the Olympic Games or the Commonwealth Games are staged in Canada it is essential to have up-to-date assessments of terrorist techniques and possible sources of attack. In crisis situations such as hijackings of aircraft or kidnappings, intelligence is needed on the character and methods of terrorists to guide those who are dealing with the situation. Furthermore, Canada, as a signatory to several international conventions concerning international cooperation in combatting terrorism (most recently the Bonn convention of 1978), is obliged to contribute to the international pool of intelligence about terrorists.

12. The third category of activity about which Canada should have security intelligence is domestic subversion. This term must be very carefully defined. If it is used loosely so as to embrace the legitimate political dissent which is the life blood of a vibrant liberal democracy, the gathering and dissemination of security intelligence will impair rather than secure Canadian democracy.

13. The key element in the subversive activity which is a *proper* subject of security intelligence activity is the attempt to undermine or attack through violence or unlawful means, the basic values, processes, and structures of democratic government in Canada. Using legal means to advocate radical change in social practices or economic relationships, or in the Canadian Constitution, must not be considered a subversive activity. Strong dissent from the *status quo* is not a category of activity about which security intelligence

should be collected; nor is the planning and carrying out of political demonstrations and processions which, although they may involve violations of local by-laws and confrontations with law enforcement officials, are not aimed at destroying fundamental elements of Canadian democracy. However, a group's activities are subversive if it aims at preventing other Canadians from enjoying such democratic rights as the right to express publicly and disseminate political opinion or the right to assemble peacefully for political purposes, or if its activities are directed towards destroying the process of democratic elections, the functioning of parliamentary institutions, adjudication by independent courts of law, or the peaceful negotiation of constitutional differences. Advance intelligence about such activities should be available to governments and to police forces.

14. Fortunately, in Canadian history political organizations on the extreme left or the extreme right have not posed a significant threat to Canadian democracy. In recent years, there has been a splintering and factionalization of groups committed to various versions of Marxism and Leninism. Most of these groups are small and appear to have no viable programmes for carrying out their anti-democratic objectives. While such groups may obtain a good deal of publicity for their totalitarian philosophies, they have not succeeded in attracting the allegiance of significant numbers of Canadians. On the extreme right, there has been an even more substantial decline in the significance of Nazi- or Fascist-type groups since pre-World War II days. Their activity in Canada today consists mostly of racist propaganda and local vandalism — activities which can, for the most part, be effectively dealt with by local police.

15. Although anti-democratic groups on the extreme right and left do not at present pose a significant threat to Canadian democracy, there is a need to keep track of their strength and of their public espousal of anti-democratic political programmes. It is also essential to detect attempts by foreign powers to use such organizations for foreign intelligence purposes. Canadians should not forget the evidence reported by the Taschereau-Kellock Royal Commission in 1946 as to the way in which the Soviet Union recruited Canadian espionage agents through the Labour Progressive Party. Security intelligence about members of organizations committed to anti-democratic ideologies is also needed in the security clearance context. Immigration and citizenship authorities, as well as government departments filling positions involving access to classified information, require advice about persons who belong to such organizations — especially those whose membership is covert.

16. For purposes of analysis we have separated the kinds of activities about which security intelligence is necessary into three distinct categories. In fact there may be considerable overlap amongst these categories. A foreign intelligence agency, for instance, has been known to provide support for terrorist groups within Canada, and Canadian political organizations committed to anti-democratic ideologies have been supportive of foreign espionage activity and acts of political violence in Canada. The common element in these three categories is that each undermines Canada's capacity for democratic self-government. That is why Canada, and indeed any prudent state in today's world, needs advance security intelligence.

Alternatives to a security intelligence agency

17. We now turn to the second part of our basic question: given that Canada needs security intelligence, is there a need at the federal level for a security intelligence agency which specializes in providing security intelligence? This question is best answered by considering the principal alternatives.

18. One alternative is to leave it to those government departments which need advice on security threats to gather the intelligence about such threats themselves. Federal and provincial immigration authorities might collect intelligence about the possible threat to Canada's internal security of applicants for immigration visas, the Department of External Affairs would be responsible for keeping track of the activities of foreign intelligence agents in Canada, the Canadian Armed Forces would collect what intelligence they need about internal threats to defence bases, government departments filling Public Service positions requiring access by the employee to secret information would secure their own information about the applicant's membership in subversive political organizations, and so on. We think this alternative would be highly impractical. It would entail the proliferation of a number of investigative agencies, each of which would have to develop the expertise required to detect the often very secretive and professional tactics of foreign intelligence agencies or to penetrate the tight security maintained by terrorist cells. This proliferation of security intelligence agencies would also have the effect of depriving Canada of a central agency for carrying out international liaison, to which foreign intelligence agencies might entrust intelligence pertaining to the internal security of Canada. Besides reducing effectiveness in intelligence gathering, this alternative would increase problems of accountability and control of intrusive intelligence collection activities.

19. The other alternative which is more frequently urged is to blend security intelligence responsibilities into the regular work of national, provincial and municipal police forces. In discussing this alternative we should make it clear that we are not considering here whether a security intelligence agency should take the form of a special division of a police force. We now have a security intelligence agency at the federal level organized as a special division of our national police force — namely the R.C.M.P. Security Service. Later we shall have much to say about whether this organizational structure should be maintained or whether the Security Service should be separated from the R.C.M.P. Here we are concerned with the more elementary and radical possibility of doing without a security intelligence agency altogether, and relying on regular police activity to provide at least the raw information upon which security intelligence is based.

20. We think it would be a serious mistake to adopt this alternative in Canada. Such an approach completely ignores fundamental differences between most police work and security intelligence responsibilities. These differences have led over the years to an increasing specialization of personnel and organizational distinctiveness of the part of the R.C.M.P. devoted to security intelligence work. The main product of security intelligence work takes the form of advice to both government and regular police forces. The ingredients of

this advice are twofold: first, the raw information obtained through investigations, and second, an analysis of the information based on an assessment of its significance in both a national and international context. The basic stages of the intelligence cycle — the selection of targets, the collection of information, its analysis and the writing of intelligence reports — require a *combination* of specialized investigative and intellectual skills that are not found in regular police forces.

21. The combination of investigative and analytical skills is an essential feature of a security intelligence agency. It would, we believe, be a serious mistake to assign the investigative and analytical roles to two different agencies. Analysis is required in the investigative process if the subjects of investigations are to be selected intelligently and the behaviour of what is observed is to be intelligently reported. In addition to the analytical and research capacity of the security intelligence agency, there is a need for government to have an analytical capacity independent of the agency to receive its reports, to integrate these reports with information obtained from other departments and to ensure that the legitimate intelligence needs of government departments are being met. But such a second level analytical bureau cannot be a substitute for research and analytical strength in the security intelligence agency itself.

22. Also, we must stress the extent to which security intelligence work must be directed by political judgment. The political judgment must be sensitive not only to the nature of security threats but also to Canada's international relations and to the civil liberties of Canadians. For instance, decisions which concern the investigation of foreign diplomats in Canada, or assessments of security risks associated with political refugees, or the choice of countries with which it is appropriate to trade intelligence, must all take Canadian foreign policies into consideration. Those involved in these decisions must have close and effective working relationships with the Department of External Affairs and the Canadian Employment and Immigration Commission — relationships which would be much more difficult to maintain if this work were distributed amongst Canadian police forces. In the area of domestic subversion, we have already stressed the need to confine security intelligence collection to a very carefully defined category of political behaviour which constitutes a genuine threat to the democratic process in Canada. The protection of civil liberties requires that the collection of intelligence in this area, particularly when intrusive techniques are involved, be subject to a thorough system of controls and independent review. The effectiveness of the system of controls and review (which we will be recommending later in this part of our Report) would be very much reduced if this function were carried out by a number of police forces.

23. Another characteristic of security intelligence work which makes it inappropriate for regular police forces is the long-term nature of many security threats. Espionage networks and terrorist support systems, for instance, may develop slowly over a long period of time, during which there is no evidence of a probable crime. It is unlikely that regular police forces in Canada, local or national, would deploy the resources required to keep such developments under surveillance for extended periods of time. We think the security of Canada

would be ill-served if there were no surveillance of these developments until a crime were about to occur or had occurred, since it would then be too easy for foreign intelligence agencies and terrorist organizations to establish a firm footing in Canada.

24. Finally, while we are convinced that national security is not an exclusively federal responsibility, we are equally convinced that there is a need for a strong security intelligence agency at the federal level of government in Canada. Certainly the provinces and their police forces have an important role to play in protecting what we have defined as the security of Canada. Provinces are concerned about securing the democratic processes of municipal and provincial government. They have a vital stake in the protection of installations such as nuclear power stations and a responsibility for protecting visiting representatives of foreign countries. When activities threatening the security of Canada reach the point of actual crime, for instance when terrorist acts occur, provincial and municipal police forces have the leading role to play in responding to the crime. In these and many other areas of security concern there is a very great need for effective provincial participation in protecting national security. But provincial contributions to Canada's internal security, however essential, cannot remove the need for an effective security intelligence agency at the federal level.

25. It is difficult to think of a serious threat to the security of Canada that does not have both national and international dimensions. This is certainly true of politically motivated terrorist organizations whose agents or supporters have been active in Canada and of organizations committed to the use of violence to change our system of government. Clandestine activities of foreign intelligence agencies are directed by foreign powers against Canada as a nation. The organization with the prime responsibility for collecting intelligence about such activities must operate across Canada on a national basis and have access to international sources of information.

26. It is important to stress the need for, and problems associated with, obtaining information about security threats from foreign sources. Many of the activities which threaten Canada's internal security have their origin in foreign countries. Canada cannot afford to be cut off from international information about threats to its security. Such information is not easily obtained. Canada requires a national security intelligence agency which is sufficiently respected internationally to obtain from the intelligence agencies of foreign countries such security intelligence pertinent to Canadian interests as may be in their possession. Without the ready co-operation of such agencies and their willingness to be forthcoming with such intelligence, the ability to protect Canada's internal security would be hobbled. Because of the sensitivity of such intelligence, foreign agencies would be unwilling to pass it to a proliferation of Canadian agencies. It is also essential that Canada's security intelligence agency be sufficiently accountable to government to ensure that the arrangements it enters into to obtain information from foreign intelligence agencies are in accord with Canada's international policies, and adequately protect the rights and interests of Canadian citizens.

27. Thus, we conclude, for all of the reasons advanced above, that it is necessary to maintain a security intelligence agency at the federal level of government in Canada. A national security intelligence agency must be a central element in Canada's security plan for the future.

B. ESSENTIAL CHARACTERISTICS OF A SECURITY INTELLIGENCE SYSTEM

28. Before we embark on a detailed discussion of each part of our proposed security plan for the future, we will provide a brief overview of the entire plan. The elements of the plan interlock and the merits of each cannot be assessed in isolation. For instance, whether or not to assign certain tasks to a security intelligence agency depends in part on the qualities of its personnel, just as the decision to give the agency certain investigative powers depends on the controls over the use of such powers. In developing our proposals we have tried to provide for a coherent system of laws, policies and procedures in which the merit of each part can best be judged by its contribution to the whole. Thus, we think it useful to set out at the beginning a brief survey of our proposed system.

29. Our conception of the functions of a Canadian security intelligence organization follows logically from our analysis of the need for a security intelligence agency at the federal level in Canada. Its basic functions should be to obtain information about threats to the security of Canada, assess and analyze that information and report intelligence about the threats to appropriate government and police authorities. More specifically, the threats about which it should collect and report intelligence are those which arise from the clandestine activities of foreign intelligence agencies in Canada, from international and domestic terrorist groups, and from organizations whose objective it is to destroy Canadian democracy. The primary functions of the security intelligence agency recommended are the collection and reporting of intelligence. The agency's purpose is to provide those with executive responsibilities — police forces or government departments — with advance intelligence about threats to security, rather than to enforce security measures by executive actions of its own.

30. The intelligence collected by the security intelligence agency must combine information obtained from relatively open sources with information that can be obtained only by covert and undercover techniques. It should be able to make good use of the best sources of public information available on the international and national contexts of security threats. It should not see itself as an investigative agency which attaches significance only to information obtained through secret means. But because the most serious immediate threats to Canada's security, especially those stemming from foreign intelligence and terrorist activities, are carried on in a highly secretive fashion, the security intelligence agency must be able to use, under proper controls, techniques that will enable it to obtain information about secret activities. These techniques should include surreptitious physical surveillance, secret informants, various forms of aural and visual surveillance, the interception of mail, the surreptitious search of private premises and access to confidential

personal information in government files. All of the security intelligence agency's methods of intelligence collection must be provided for by law and subject to effective mechanisms of control and review.

31. The security intelligence agency should rely primarily on liaison with foreign intelligence agencies for obtaining information about secret activities abroad which threaten Canada's security. For this purpose the agency should be permitted to enter into intelligence-sharing arrangements with foreign agencies. But these arrangements must be subject to thorough government scrutiny to ensure that they are consistent with Canada's international policies and democratic values. On rare occasions, in order to obtain information important for Canada's security, it may be necessary for the security intelligence agency to collect information outside Canada through its own sources. Where this is essential, the agency should be permitted to function abroad subject to a system of government control which takes into account both Canada's security needs and international policies. There is a need for strict limitations and controls on these activities. We discuss them in Chapter 7 of this Part.

32. To fulfill its role effectively Canada's security intelligence agency will need strength in both investigation and analysis. The judgment and skill involved in deciding which subjects should be investigated, and in assessing the significance of information and reporting it in a useful way to government, require personnel recruited from diverse backgrounds. The training and continuing education of the personnel of the security organization must emphasize an understanding of, and loyalty to, the democratic system which it is the aim of the security organization to secure, as well as a firm grounding in the craft of counter-intelligence and the skills of analysis. The personnel of the security intelligence agency must not be split into first-class and second-class citizens: analytical strength must be possessed by its intelligence officers at all levels of the organization, and must not be a specialty of a small, isolated group.

33. Retaining and melding such personnel into an effective team will require management policies which emphasize collegiality rather than hierarchy, and are designed to establish an internal environment in which respect for legality and propriety is a governing norm. Well-informed but independent legal advice must be easily accessible. The organization must have an effective system of internal security and the capacity to detect and prevent penetration attempts by hostile agencies. To obtain the desirable diversity of outlook and the range of talent, senior management should include persons with experience in various sectors of private and public life. Given the organization's responsibility to provide timely and useful advice to government, its members must be well-equipped to deal with government, and adept at interpreting its intelligence needs. At the same time they must have a sufficient understanding of our constitutional system to be able to recognize and resist improper government direction.

34. An organization with the personnel, management and relationship to government which we think are desirable for an excellent security intelligence service is not, in our view, likely to be developed and maintained within the

R.C.M.P. Therefore we shall be recommending that the security intelligence agency be separated from the R.C.M.P. but kept under the direction of the same Minister, the Solicitor General of Canada, who is responsible for the R.C.M.P. The Canadian security intelligence agency, like similar organizations in Australia, New Zealand and the United Kingdom, should not have police powers. When it determines that its investigations will lead to arrests and prosecutions it should turn to the police and prosecutorial authorities for action. Thus effective liaison must be maintained between the security intelligence agency and police forces, both national and local, to facilitate cooperation and avoid duplication.

35. The agency should be established by an Act of Parliament. That Act should define the organization's mandate, its basic functions, its powers and the conditions under which they may be used, and its organizational structure. It should also provide for its direction by government and for independent review of its activities. The statutory definition of its mandate should define the types of activity constituting threats to the security of Canada to which the intelligence collection work of the agency must be confined. There must be no undisclosed additions to this mandate by the agency itself or by the executive branch of government, whether such additions be inadvertent or deliberate.

36. Security screening programmes for Public Service employment, immigration and citizenship should not assign intelligence collection tasks to the security intelligence agency which may be outside its statutory mandate. Thus, it is important to ensure that the definition of threats to the security of Canada in the laws and administrative directives governing these programmes is consistent with the definition of threats to the security of Canada in the statute governing the security agency. Further, the security screening programmes should be more carefully managed and monitored so that they are confined to areas where they are really necessary and to ensure that they are effective in those areas. Poor administration of security screening programmes will have the undesirable consequence of unnecessarily expanding the scope of security service investigations into the personal backgrounds of individuals.

37. In addition to its role in providing security intelligence about individuals for security clearances, the agency should also have the function of providing advice to government departments and police forces responsible for maintaining physical security. This means, among other things, that as a source of accurate and timely intelligence on activities threatening the security of Canada the agency should play an important role in protective security programmes for the protection of vital points and the protection of V.I.P.s. In emergency situations, involving foreign military threats to Canada or grave political violence, the agency must also be an effective source of intelligence on individuals or groups who threaten the internal security of the country. But it is also essential that the procedures and laws which govern such emergencies entail the minimum encroachment on civil liberties consistent with effective security. For this purpose, we will be recommending amendments to the War Measures Act and changes in the draft internal security regulations.

38. Overall responsibility for overseeing the implementation of the security organization's statutory mandate should rest with the Prime Minister and the Cabinet. It is the function of the Cabinet to establish the intelligence priorities for the security intelligence agency and other departments or agencies of the federal government which have intelligence collection responsibilities. Modifications in the system of interdepartmental committees centred on the Privy Council Office are needed to assist the Cabinet in establishing security policy, in coordinating intelligence collection activities, and in ensuring that intelligence which is collected is assessed and put to good use by government departments.

39. Ministerial direction of the security intelligence agency should be the responsibility of the Solicitor General of Canada. The Solicitor General should be responsible both for ensuring that the Cabinet's policies with respect to the agency are carried out and for submitting proposals for new policies to Cabinet. The Minister's responsibility for policy must extend to the policy of operations. He must have knowledge of all investigative techniques and liaison arrangements. Difficult or sensitive operational decisions must not be kept from the Minister but, on the contrary, brought to him for decision and, if necessary, taken by him in turn to the Prime Minister or Cabinet. To carry out these responsibilities, Solicitors General must have the assistance of well-informed senior officials who are not themselves members of the security organization. Thus, the Deputy Solicitor General must have the full powers of a Deputy Minister in relation to the agency.

40. One of the Solicitor General's major responsibilities should be to establish and maintain procedures for ensuring effective cooperation between federal, provincial and municipal authorities with respect to national security matters. Regular briefings of provincial attorneys general and solicitors general should be arranged. The Solicitor General of Canada should in this forum seek the agreement of the provincial governments to propose to the respective provincial legislatures changes in provincial laws required to ensure that undercover investigations essential for the security of Canada can be carried on without violating provincial statutes.

41. The security intelligence agency's determination of the subjects about which it should collect information and make intelligence reports must be guided by the intelligence priorities set by the Cabinet. The Cabinet's identification of general areas of interest and the security agency's choice of specific 'targets' must fall within the categories of activities which Parliament has presented as proper subjects for the security agency's surveillance. The security agency should be willing and able to ascertain the security implications of many phenomena by using public sources of information. Decisions to use investigative techniques which entail surreptitious methods, or methods which invade individual privacy, should adjust the intrusiveness of the technique in proportion to the danger of the threat, and the more intrusive the technique the more senior should be the person or committee required to approve its use.

42. A decision-making system, with special provision for emergency situations, must be established which ensures that investigations involving the most

intrusive techniques of investigation, deep cover human sources and undercover agents, the interception of private communications and the surreptitious entry and search of premises must be undertaken only after approval by the Director General of the agency and the Solicitor General and on the basis of well-defined standards of necessity. There must also be provision for ensuring that the legality of proposed investigations is reviewed by a member of the Department of Justice and that the Department of External Affairs is consulted on investigations affecting foreigners or foreign missions in Canada. In addition to ministerial approval, the use of certain aural and visual surveillance techniques, mail checks, surreptitious entries of private premises and access to confidential personal information in government files should require judicial warrants. The role of the judge is to ensure that the standard set down by statute for the use of these techniques has been met.

43. The thoroughness of ministerial direction and control of security intelligence activities which our proposals call for raises the danger of improper political or personal use of the security intelligence agency. Our democratic system of government would be endangered if the 'targets' of security investigations were selected or vetoed for partisan political reasons or for personal reasons. To guard against this possibility, the Director General should have by statute some security of tenure for his term of office, and he should have direct access in urgent situations to the Prime Minister and to an independent review body. Also, the leaders of parliamentary parties should be consulted on the appointment of the Director General.

44. A constant and thorough review of the efficacy, legality and propriety of security intelligence operations must be carried out by the Director General and senior management of the agency itself. It is especially important that investigations be carried out for limited time periods and that a careful assessment be made of an investigation's contribution to the security of Canada. The Solicitor General should not authorize the extension of an investigation beyond a year, unless he is satisfied that it is likely to yield essential security intelligence. The Prime Minister and Cabinet should also receive, on no less than an annual basis, a report of the agency's activities. This report should indicate the extent to which the security intelligence agency has met the government's security intelligence requirements and any problems it has encountered. These reports should serve as a basis for the Cabinet's reassessment of those requirements.

45. Just as it is essential to maintain a thorough review of security intelligence activities on the executive side of government, it is also crucial to have independent review, both parliamentary and non-parliamentary. The secrecy of intelligence operations, their lack of exposure to judicial examination and comment, the danger to civil liberties of excessive surveillance, and the record of past wrong-doings, all point to the need for an effective review of security operations by persons independent of the government of the day. For this reason we will be recommending the establishment of an independent review body with complete access to all of the security intelligence agency's records. This body, which we suggest might be called the Advisory Council on Security and Intelligence, would carry out a continuous *ex post facto* review of the

agency's activities, focussing on their legality and propriety. It would have no executive powers but would report on an advisory basis to the Solicitor General. It would also report to a joint standing committee of Parliament and, at least annually, issue a public report. The Advisory Council on Security and Intelligence should assist the Solicitor General in providing opportunities for wider public discussion and study of security problems than has occurred in the past.

46. Parliament requires an enhanced capacity to scrutinize security and intelligence activities. The necessarily secret nature of these activities makes it impossible for Parliamentary scrutiny to be exercised effectively through any mechanism other than a small committee whose members either include the party leaders or are specially selected by them. This committee's effectiveness will depend on its capacity to develop and maintain the confidence of all parliamentary parties, as well as that of the government and the security agency. The scope of the scrutiny exercised both by the Joint Parliamentary Committee on Security and Intelligence and by the Advisory Council on Security and Intelligence should extend to the activities of all those intelligence collecting agencies and departments of the federal government whose activities involve the use of covert techniques of investigation. If independent and parliamentary review focusses solely on the security intelligence agency, there is a danger that a government might, wittingly or unwittingly, circumvent this scrutiny by assigning surveillance tasks to other agencies.

47. In the field of security screening, where individual rights are directly affected by government decisions based on security intelligence reports and the individual does not have access to his security file, a review body is needed to provide some assurance of fair and reasonable treatment. This body should be independent of the government of the day. Because it will be dealing with individual cases on an advisory basis it should operate as a tribunal and be separate from the Advisory Council on Security and Intelligence. The scope of the security tribunal's review should extend to security screening cases with respect to Public Service employment, immigration and citizenship.

48. The paragraphs above describe what might be termed the bare essentials of our security plan for the future. Every point, every proposal requires detailed elaboration and reasoned defence. In what follows we will endeavour to provide just that. But we urge that in assessing each of the detailed proposals which follows there be kept in mind the security system as a whole and the extent to which it can coherently meet *both* the requirements of security and the requirements of democracy.

CHAPTER 3

THE SCOPE OF SECURITY INTELLIGENCE

INTRODUCTION

1. The first task we face in defining the functions of a security intelligence agency is to identify the categories of activity about which the agency should be permitted to collect, analyze and report intelligence. The identification of security threats which constitute the proper subjects or 'targets' of security intelligence operations provides one component of what might be called the security agency's 'mandate'. It is this aspect of the mandate which we deal with in this chapter. In subsequent chapters we deal with two other elements of its mandate, namely the methods it uses to collect intelligence and what it does with the intelligence it collects.

A. A STATUTORY DEFINITION OF SECURITY THREATS

2. The current mandate of the R.C.M.P. Security Service is diffuse and ambiguous. It is not clearly provided for in law. The security intelligence functions of the R.C.M.P. are not explicitly and comprehensively set out in an Act of Parliament, Order-in-Council or administrative directive. Over the years security intelligence functions have been assigned to the R.C.M.P. by ministerial correspondence (for example, in citizenship vetting) and by Cabinet directive (for example, Cabinet Directive 35 governing security screening in the Public Service). Sometimes functions have been assigned by decisions of committees of senior officials (for instance, the Security Advisory Committee's decision that the Security Service should provide information about the separatist associations of persons applying for security clearance). Functions were also assumed by the Security Service when its members, on the basis of general policy positions adopted by the government, inferred that they were to carry out those functions (for example, disruptive tactics).

3. It was not until March 1975 that a Cabinet Directive entitled "The Role, Tasks and Methods of the R.C.M.P. Security Service" was issued. This Directive was far from comprehensive: it did not mention a number of the then current functions of the Security Service, some of which, for instance its role in security clearance programmes, required the Security Service to collect information about activities not covered by the Directive. Similarly the methods and powers used by the R.C.M.P. Security Service to investigate and counter threats to security were not clearly and comprehensively set out in either law or

directive. It is our firm conviction that this situation should not be permitted to continue. The functions of the security intelligence agency and the powers and methods it may use in carrying out those functions must be explicitly, coherently and comprehensively stated.

4. We believe that the definition, by several categories, of the activities about which the agency should be authorized to collect, analyze and report intelligence should be established by Act of Parliament. Such a definition would not refer to specific groups or activities. Its purpose would be to fix the boundaries of security intelligence activities. We believe it is essential to set these boundaries in legislation. This statutory definition of the limits of security intelligence operations should express Parliament's will as to the kinds of political activities it regards as threats to the security of Canada and therefore as the proper subjects of security intelligence surveillance.

5. Past experience has demonstrated the dangers involved in leaving the definition of these limits to the discretion of the government or to the security agency itself. In the past, as our examination in section B of this chapter will show, neither the government nor the R.C.M.P. has had clear and consistent policies on the proper limits of security intelligence investigations. As a result R.C.M.P. surveillance on occasion went beyond the requirements of the security of Canada. Of equal concern is the fact that on other occasions it may have fallen short of what was required to meet Canada's security needs. Therefore, we think that whether the security intelligence functions continue to be the responsibility of the R.C.M.P. Security Service or are assigned to a separate civilian agency, their proper limits should be defined by an Act of Parliament.

6. In proposing statutory limits on security intelligence surveillance, we must acknowledge that when the security intelligence agency begins to collect information on a subject it cannot always be expected to know, or to have reason to believe, that a particular individual or group is in fact engaging in one of those activities defined by Parliament to be a proper subject of security intelligence surveillance. In the next chapter we shall consider and make recommendations with respect to the full range of intelligence collection techniques, from open sources, such as the media, books and public meetings, interviews, casual sources, and reports from other agencies, to the more intrusive techniques of physical surveillance, paid informants, undercover agents, certain aural and visual surveillance techniques, surreptitious entry, mail checks and access to confidential personal information in government files. A basic principle in the system of controls we shall propose for the use of these techniques is that the more the use of a technique encroaches on individual privacy and freedom of political association and of speech, the stronger the evidence should be of a significant threat to the security of Canada. To use a shorthand phrase: the more intrusive the technique, the higher should be the threshold. When the security intelligence agency begins to take an interest in a subject through information obtained by collection techniques at the least intrusive end of the spectrum, it need have only minimal evidence on which to base its suspicion. Its interest might be triggered by newspaper reports or a tip received from a police force or a foreign agency: all

that can be required initially is that the activity which the agency suspects an individual or group may possibly be involved in is within the categories of activity defined by Parliament to constitute threats to national security.

7. The statutory definition of security threats should be designed to identify at the most general level the activities which *may* be lawfully investigated by the security intelligence agency. Within these statutory limits the Cabinet should be responsible for determining the principal areas of activity about which the government *requires* intelligence. The Cabinet should establish intelligence requirements, thus indicating the foreign and domestic threats which are of greatest concern to it. While the security intelligence agency's assessment of intelligence threats will be an important factor in the Cabinet's determination of its intelligence requirements, the Cabinet should have the fundamental responsibility for establishing these requirements. (In Part VIII of this Report we shall make recommendations about the process of determining intelligence requirements at the Cabinet level.) Within the general statutory limits defined by Parliament, and following the more specific designation of areas of concern by the Cabinet, the security intelligence agency should identify the particular individuals and groups of security interest.

8. Thus we envisage a three-step process in discerning or identifying threats to the security of Canada. At the level of greatest generality, the Act establishing the security intelligence agency should contain the legislative framework within which all security operations are conducted, and should set out the definitions of threats to the security of Canada. At a somewhat more specific level, constituting the highest level of government direction of the security agency, are the intelligence requirements of the Government of Canada as determined from time to time by the Cabinet. Finally, at the most specific level, are the decisions of the security intelligence agency to 'target' particular groups or individuals. When the latter decisions entail the use of the more intrusive techniques of investigation, ministerial approval and, with regard to certain techniques, judicial authorization should be obtained. We will be setting out our proposals with regard to controls of these intrusive techniques in the next chapter.

9. The system we have described above expresses our general expectation of the roles to be played by Parliament, Ministers and the security intelligence agency itself. The three stages of decision-making we have identified should not be regarded as water-tight compartments: there must be a good deal of interaction among those involved at the different levels. At the outset, this system will no doubt require some adjustments before it functions in a manner which effectively reconciles efficiency with the requirements of responsible government.

10. In recent years a number of western democracies have defined more precisely the kinds of activities about which their security intelligence agencies should collect and report information. Some have done this by Act of Parliament, notably Australia and New Zealand. Others have proceeded by way of administrative guidelines issued by the Minister responsible for the security agency (for example, Great Britain and the United States), or by an executive

order of the government (for example, the Netherlands) or a Cabinet Directive, as in the case of Canada.

11. In Canada, Cabinet Directive of March 27, 1975, on the "Role, Tasks and Methods of the R.C.M.P. Security Service", lists six kinds of activities which the Security Service is authorized to "discern, monitor, investigate, deter, prevent or counter". These are:

(i) espionage or sabotage;

(ii) foreign intelligence activities directed toward gathering intelligence information relating to Canada;

(iii) activities directed toward accomplishing governmental change within Canada or elsewhere by force or violence or any criminal means;

(iv) activities by a foreign power directed toward actual or potential attack or other hostile acts against Canada;

(v) activities of a foreign or domestic group directed toward the commission of terrorist acts in or against Canada; or

(vi) the use or the encouragement of the use of force, violence or any criminal means, or the creation or exploitation of civil disorder, for the purpose of accomplishing any of the activities referred to above.

This list of 'targettable' activities corresponds closely to the activities listed in section 16(3) of the Official Secrets Act which came into effect on July 1, 1974. That section defines "subversive activity" in relation to which the interception and seizure of private communications may be authorized by the Solicitor General of Canada. The 1975 Cabinet Directive adds the activities of *domestic* terrorist groups in paragraph (v) and the activities leading to civil disorder referred to in its sixth paragraph.

12. We have studied the ways in which the 1975 Cabinet Directive and section 16(3) of the Official Secrets Act have been interpreted. We have also examined the definitions and guidelines developed by a number of other democratic countries. On the basis of our examination of Canadian and foreign experience and our consideration of Canada's needs we shall now identify the activities about which a security intelligence agency should be authorized to collect, analyze and report intelligence.

Espionage and sabotage

13. One of the most important functions of a security intelligence agency is to obtain information about efforts to conduct espionage and sabotage against Canada. The emphasis in the agency's mandate on this subject should be to detect activities that are preparatory to actual espionage or sabotage. Actual acts of espionage and sabotage often occur when a foreign power has succeeded in secretly obtaining the services of a government employee in a sensitive position. Clearly, the security intelligence agency should try to detect these recruitment activities at the earliest possible stage. Similarly, the security of Canada requires the detection of foreign agents who may try to remain undercover for many years with the objective of participating in espionage or

sabotage only in the event of hostilities. In the process of investigating suspected foreign agents, the security intelligence agency may uncover actual acts of espionage or sabotage in which case it may bring the matter to the attention of appropriate law enforcement officials or, in the case of persons with diplomatic immunity, to the attention of the Department of External Affairs. But the principal objective of the agency should be to detect espionage and sabotage efforts before offences occur.

14. The words 'espionage' and 'sabotage' are not defined in either the 1975 Cabinet Directive or section 16(3) of the Official Secrets Act. We think that where these words are used to define activities which may be investigated by the security intelligence agency, they should be given the meaning which they have under the statutes dealing with the offences of espionage and sabotage.

15. The word 'espionage' is not used in the Criminal Code, but section 46(2)(b) of the Criminal Code provides that:

> Everyone commits treason who, in Canada, . . .
>
> (b) without lawful authority, communicates or makes available to an agent of a state other than Canada, military or scientific information or any sketch, plan, model, article, note or document of a military or scientific character that he knows or ought to know may be used by that state for a purpose prejudicial to the safety or defence of Canada.

Another statutory offence which is a form of spying is defined in section 3 of the Official Secrets Act as follows:

> 3. (1) Every person is guilty of an offence under this Act who for any purpose prejudicial to the safety or interests of the state,
>
> (a) approaches, inspects, passes over, or is in the neighbourhood of, or enters any prohibited place;
>
> (b) makes any sketch, plan, model or note that is calculated to be or might be or is intended to be directly or indirectly useful to a foreign power; or
>
> (c) obtains, collects, records, or publishes, or communicates to any other person any secret official code word, or password, or any sketch, plan, model, article, or note, or other document or information that is calculated to be or might be or is intended to be directly or indirectly useful to a foreign power.

In our First Report we recommended that there be new legislation incorporating in a single enactment the offences now set out in section 3(1) of the Official Secrets Act and section 42(2)(b) of the Criminal Code. We also recommended that the offence of 'harbouring' espionage agents be more carefully defined and that possession of the tools of espionage, without lawful excuse, be made a criminal offence. We think the implementation of these recommendations will bring greater clarity and precision to the identification of activities falling under this component of a security intelligence agency's mandate.

16. Similarly, in relation to sabotage we recommended in our First Report elimination of the "prohibited place" provisions of the Official Secrets Act, leaving the sabotage section of the Criminal Code to cover activities threaten-

ing defence installations. The sabotage section of the Criminal Code is section 52 which makes it an offence to do

> a prohibited act for a purpose prejudicial to
>
> (a) the safety, security or defence of Canada, or
>
> (b) the safety or security of the naval, army or air forces of any state other than Canada that are lawfully present in Canada.

Section 52(2) defines "prohibited act" as meaning

> An act or omission that
>
> (a) impairs the efficiency or impedes the working of any vessel, vehicle, aircraft, machinery, apparatus or other thing, or
>
> (b) causes property, by whomsoever it may be owned, to be lost, damaged or destroyed.

It is in the sense of this definition in the Criminal Code rather than in any colloquial or dictionary sense that the term "sabotage" should be understood and used by a security intelligence agency.

Foreign Interference

17. Espionage and sabotage are not the only kinds of foreign directed activities which should be monitored and investigated by a security intelligence agency. Foreign governments and foreign political organizations may in a clandestine manner try to interfere in Canadian political life. Programmes of secret political interference by foreign intelligence agencies are sometimes referred to as "active measures" (a Russian term) or "covert action" (an American term). The latter was defined (with reference to U.S. foreign intelligence agencies) by the Church Committee as:

> ...Clandestine activity designed to influence foreign governments, events, organizations or persons in support of U.S. foreign policy conducted in such a way that the involvement of the U.S. Government is not apparent. In its attempts directly to influence events it is distinguishable from the clandestine intelligence gathering — often referred to as espionage.[1]

As this definition makes clear, deception is an essential feature of "active measures" or "covert action". Diplomatic and military measures can be used against open attempts by foreign powers to interfere in Canadian affairs. A security intelligence agency is necessary to warn government of clandestine programmes of foreign intervention.

18. Active measures of foreign interference are effected in many different ways. Sometimes a member of an ethnic community is forced by a foreign diplomat to support the government of the country from which the person emigrated through threats of harm to family or friends who live in that country. Covert interference may also take the form of secretly employing a Canadian government official to support a foreign government's interests. Yet

[1] U.S. Senate, *Final Report of the Select Committee to Study Government Operations with Respect to Intelligence Activities*, Book 1, U.S. Government Printing Office, Washington, 1976, p. 131.

another variation would be the secret funding by a foreign government of a political party, movement or group in Canada. Foreign powers may also use covert means to obtain technological information from both the public and private sectors. There is evidence on the public record that the carrying out of active measures or covert actions is part of the mandate of foreign intelligence agencies of a number of major powers, Communist and non-Communist. There is no reason to believe that Canada has been or would be declared "off-limits" for these activities.

19. While we think it should be part of a security intelligence agency's mandate to keep governments in Canada informed of these activities, we also think it important that the agency should distinguish generally acceptable diplomatic, commercial and cultural activities of representatives of foreign powers in Canada from activity which constitutes an improper interference in Canadian political life. The ability to make this distinction will depend to a large extent on the agency's analytical capabilities and political understanding, as well as on the assistance it receives from the Department of External Affairs. In our First Report we said we would give consideration to the establishment of a system requiring the registration of all agents of foreign governments, thus making it an offence to operate as an unregistered agent, or the enactment of a provision which would make it an offence to be the secret agent of a foreign power. While proposals of this kind might provide a firmer legal basis for identifying foreign interference activities, for reasons which we set out in Part IX, Chapter 3 of this Report, we have concluded that it would not be wise to introduce either of these changes into Canadian law.

20. To define the scope of the security intelligence operations in relation to this kind of security threat we favour the language used in the Australian Security Intelligence Organization Act of 1979. Section 4 of that Act defines "active measures of foreign intervention" as follows:

> clandestine or deceptive action taken by or on behalf of a foreign power to promote the interests of that power;

This definition has the merit of identifying the two distinctive features of the foreign interference which we consider to be a proper subject for security intelligence surveillance: their covert nature and their purpose. It should be noted that this definition would justify surveillance of covert acts of foreign agents in Canada which may not be primarily directed *against* Canada but are designed to promote the interests of a foreign power.

21. We think the above definition used in the Australian Act is to be preferred to the language now used in the 1975 Cabinet Directive and in section 16(3) of the Official Secrets Act, in both of which the second and fourth clauses read as follows:

> (ii) foreign intelligence activities directed toward gathering intelligence information relating to Canada;
>
> (iv) activities by a foreign power directed toward actual or potential attack or other hostile acts against Canada.

22. The first of these two clauses, clause (ii), is too narrow in one sense and too broad in another. It is too narrow in that it might be interpreted as

referring only to intelligence collection activities of foreign powers in Canada and to exclude political interference. It is too broad in that it would appear to embrace the collection of intelligence about Canada by agents of foreign powers by open and public means as well as by covert means.

23. The second clause, clause (iv), strikes us as unnecessary. An early draft of a 1978 Security Service discussion paper interpreting the 1975 Cabinet Directive referred to this paragraph as a 'catch-all' designed to refer to "the wide variety of 'hostile acts'... only limited (by) the scope of the reader's imagination". The final version of this paper, entitled *A Discussion Paper on the Interpretation of the Security Service Mandate*, and dated October 17, 1978, gave the following four examples of activities which might come under clause (iv):

(a) encouragement and active support for actions which would undermine the unity of Canada including the secession of any Province;

(b) an attack in Canada against a person or property of another country;

(c) using Canada as a staging area for agent infiltration into another country;

(d) infringement of Canadian sovereignty or integrity including, but not restricted to, attempts by another country to maintain and exercise control over its former citizens residing in Canada.

Example (a) refers to activities which, on the basis of our understanding of the meaning of national security, should be of interest to the Security Service only if they constitute what we have defined as active measures of foreign intervention, namely clandestine or deceptive action taken by or on behalf of a foreign power to promote the interest of that power in Canada. In section B of this chapter we point out that, in the past, confusion has arisen from equating in all respects the two concepts of national security and national unity. Example (b) refers to activities which should be under surveillance by the security intelligence agency only if they constitute acts leading to sabotage or international or domestic terrorism (we will deal with these latter two concepts in the next section below). Otherwise such activities should be dealt with by the police. Examples (c) and (d) should be of interest to the agency if they involve espionage, foreign interference (as we have defined that term) or international terrorism.

24. We think it unwise to include broad 'catch-all' phrases in the security intelligence agency's mandate. We are satisfied that the four kinds of threat to the security of Canada which we shall recommend as the basis for the statutory definition of the security agency's mandate will adequately cover those activities in relation to which Canada should have security intelligence and which might have been brought under clauses (ii) and (iv) of the existing mandate. Therefore we shall recommend removing clauses (ii) and (iv) from both the mandate of Canada's security intelligence agency and from section 16(3) of the Official Secrets Act.

25. In interpreting references to "foreign power" in section 16(3) of the Official Secrets Act and in the 1975 Cabinet Directive, some doubt has been expressed as to whether a Commonwealth country should be considered

"foreign". We think that the reference to foreign interference in the legislation governing the security intelligence agency should extend to unacceptable activities on behalf of Commonwealth countries, should such ever occur.

Political violence and terrorism

26. The democratic process in Canada requires that political objectives be pursued through public discussion, legislative debate and lawful representation of interests. The democratic process is jeopardized when groups or individuals attempt to gain their political objective by threatening to carry out acts of serious violence or actually carrying out such acts. As we have explained in Chapter 1 of this part of the Report, the protection of the democratic process should be the central purpose of Canada's security arrangements. Thus, we believe that Canada's security intelligence agency should be empowered to provide intelligence about any activities of an individual or group which involve the threat or use of serious violence against persons or property for the purpose of accomplishing political objectives.

27. For more than a decade the most prominent form which this threat to security has taken is terrorism. The political fanaticism and frustration which engender terrorism are not, unfortunately, likely to disappear in the foreseeable future. As we suggested earlier in this Report, modern means of transportation, communication and destruction have increased the damage that a small group of terrorists can inflict on a large country such as Canada. We should re-emphasize here that the kind of terrorist acts which should be of concern to the security intelligence agency are those which have political objectives. Acts of violence for personal gain or by mentally disturbed persons which do not threaten the democratic process of government should be of concern to law enforcement agencies, not the security intelligence agency.

28. The security of Canada requires the detection of activities of persons who belong to or support terrorist groups before there is evidence which would support a criminal prosecution. Recent experience with terrorist groups has shown that their success has often depended on their ability to maintain their cover and security while operating in a modern community. Mr. Paul Wilkinson, an English author, has provided the following apt description of this phenomenon and the intelligence needs it generates for the contemporary liberal state:

> . . . mass support is not a prerequisite for launching a terrorist campaign. Indeed the archetypal terrorist organization is numerically small and based on a structure of cells or firing groups, each consisting of three or four individuals...
>
> ...The terrorists' small numbers and anonymity make them an extraordinarily difficult quarry for the police in modern cities, while the ready availability of light portable arms and materials required for home-made bombs makes it difficult to track down terrorist lines of supply. Yet once the key members of a cell have been identified it is generally practicable to round up other members. And on the basis of information gleaned from interrogating a relatively small number of key terrorist operatives it is possible to spread the net more effectively around the whole organization.

> A crucial requirement for defeating any political terrorist campaign therefore must be the development of high quality intelligence, for unless the security authorities are fortunate enough to capture a terrorist red-handed at the scene of the crime, it is only by sifting through comprehensive and accurate intelligence data that the police have any hope of locating the terrorists. It is all very well engaging in fine rhetoric about maximising punishment and minimising rewards for terrorists. In order to make such a hard line effective the government and security chiefs need to know a great deal about the groups and individuals that are seeking rewards by terrorism, about their aims, political motivations and alignments, leadership, individual members, logistic and financial resources and organizational structures...
>
> ...The primary objective of an efficient intelligence service must be to prevent any insurgency or terrorism developing beyond the incipient stage. Hence a high quality intelligence service is required *long before the insurgency surfaces*. It is vital moreover, that such a service should have a national remit — to avoid duplication and rivalry between area police forces — and that it should be firmly under control of the civil authorities, and hence democratically accountable.[2]

29. Accurate intelligence about terrorists is needed not only to enable the government and police forces to take effective action against them but also to avoid over-reacting to their threats. Assessments of the strength and location of terrorist groups based on sound intelligence enable the government to cope with a terrorist crisis by methods appropriate to the real rather than the imagined dimensions of the threat. A small group of terrorists could realize a very great victory for their undemocratic cause by frightening a government into adopting measures which encroach on the civil liberties of citizens to a degree far in excess of what may be necessary to deal with the actual threat.

30. The security agency's mandate should provide for the collection of intelligence about the activities of terrorists in Canada (including activities in preparation for and in support of terrorist acts) whether such activities are directed against Canadians or Canadian governments or against foreigners or foreign governments. In an era which has witnessed a startling expansion of international terrorism, Canada must not become a haven for those planning to use the methods of terrorism to gain their political ends in other countries. But it is important to distinguish international groups secretly pursuing in Canada terrorist objectives against foreign governments, from representatives of foreign liberation or dissident groups who come to Canada to promote their cause openly. This latter activity should be kept under surveillance by the security intelligence agency only when there is reason to suspect that it is accompanied by clandestine activity or may lead to serious political violence in Canada. Again we should emphasize that in distinguishing between these foreign groups good judgment, sensitive to Canada's foreign policies and democratic ideals, must be exercised.

31. The need for Canada's security intelligence agency to obtain information about foreign terrorist activities in Canada, whether or not directed against

---

[2] Paul Wilkinson, *Terrorism and The Liberal State*, Toronto, Macmillan/MacLean-Hunter, 1977, pp. 133-35.

Canada, arises not only from the requirements of national security but also from Canada's international obligations. Canada, as we mentioned earlier, is party to a number of international conventions concerning the prevention of terrorism.[3] For our purposes, the most pertinent of these is The Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents, which was adopted by consensus at the General Assembly of the United Nations on December 14, 1973. This convention covers the most serious terrorist crimes: murder, kidnapping and violent attacks or threats of violent attacks upon the official premises, private accommodation or means of transportation of "an internationally protected person" likely to endanger his or her person or liberty. Canada signed this convention in 1974 and passed implementing legislation to introduce a definition of "an internationally protected person" into the Criminal Code.[4] Article 4 of the Convention requires all contracting parties to cooperate in the prevention of these terrorist crimes by:

> (a) taking all practicable measures to prevent preparations in their respective territories for the commission of those crimes within or outside their territories;
>
> (b) exchanging information and coordinating the taking of administrative and other measures as appropriate to prevent the commission of those crimes.[5]

Canada's security intelligence agency should have the primary responsibility for supplying Canada's contribution to the information referred to in paragraph (b) of this convention. It should be noted that paragraph (a) explicitly commits contracting parties to do what they practically can to prevent these serious terrorist acts from taking place *outside* their territories.

32. Section 16(3) of the Official Secrets Act and the 1975 Cabinet Directive are both deficient in their coverage of foreign terrorist activity. Section 16(3)(e) of the Official Secrets Act refers to:

> activities of a foreign terrorist group directed toward the commission of terrorist acts in or against Canada;

Section 16(3), which provides the definition of "subversive activity" is governed by section 16(2) which empowers the Solicitor General to issue warrants for the interception or seizure of communications "for the prevention or detection of subversive activity directed against Canada or detrimental to the security of Canada". The phrase "detrimental to the security of Canada" has been interpreted by the Department of Justice as not extending to terrorist activities in Canada directed towards carrying out terrorist acts in a foreign country. The fifth paragraph of the 1975 Cabinet Directive extends the

---

[3] For an account of these conventions and Canada's participation in them see "Terrorism — the Canadian Perspective", by L.C. Green, in Y. Alexander (ed.) *International Terrorism: National, Regional and Global Perspectives*, New York, Praeger, 1976.

[4] *Statutes of Canada*, 1974-75-76, ch.93, s.2(1).

[5] *Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents*, United Nations, 1974.

Security Service mandate to domestic as well as to foreign groups and there is no clause limiting the Security Service's interest in terrorist acts to those which in the narrowest sense are detrimental to Canada's security. Still, paragraph (v) of the Cabinet Directive appears to be too narrow, as it refers only to the commission of terrorist *acts* in Canada and not to activities directed towards the commission of terrorist acts in foreign countries.

33. The statutory definition of the limits of the security agency's intelligence role should be designed to overcome these deficiencies and extend the agency's mandate clearly to activities in Canada directed toward the commission of terrorist acts in Canada or abroad against Canadians or foreigners.

34. There are activities involving the use of acts of serious violence against persons or property for the purpose of accomplishing political objectives which would normally not be described as terrorist acts. For example, political organizations which endeavour to use 'goon squads' or other strong-arm tactics to intimidate their political opponents or to break up peaceful political meetings or to turn peaceful assemblies into violent confrontations, pose a threat to the democratic process and as such should be of concern to a security intelligence agency. Or, to take another example, an organization that plans to mobilize a large group to attack physically the officials or premises of a government department in an attempt to change a particular policy also threatens the democratic system of government. It would be wrong for the security agency to treat the need for advance information about such activities as authorization for the surveillance of every group which might be suspected of initiating some act of vandalism against its political opponents. Only when the activities pose a serious threat to the basic democratic processes of public discussion and debate should they be the concern of the security intelligence agency. The responsibility for dealing with such political violence when it occurs rests primarily with locally based police forces. The security intelligence agency's role should be confined to collecting intelligence about those who appear to be organizing political violence as systematic strategy or on a very large scale or who have international sources of support.

35. The terms of the Security Service's existing mandate are poorly phrased to cover the kind of political violence which we think should be within the mandate of a security intelligence agency. Paragraph (iii) of the 1975 Cabinet Directive refers to

> activities directed toward accomplishing governmental change within Canada or elsewhere by force or violence or any criminal means;

The ambiguous words "governmental change" have been interpreted by the Security Service to include changing a government policy as well as overthrowing a government or our system of government. Thus this clause is wide enough to cover the use of violence to attain political objectives falling short of overthrowing the government or the entire democratic system. The words "force" or "any criminal means" have the potential for expanding the security agency's mandate too widely. Strikes and demonstrations, for instance, designed to bring pressure to bear on government to change a policy, might be considered to involve the use of "force". Participants in popular assemblies,

public meetings, parades and demonstrations may be guilty of violating traffic regulations, municipal by-laws and committing other minor offences. While political activities of this kind may be of concern to peace officers at the local or provincial level they should not be the concern of a national security intelligence agency, unless there is some indication of clandestine foreign interference or of deliberate attempts to turn peaceful demonstrations into violent confrontations destroying the democratic process.

36. The sixth paragraph of the 1975 Cabinet Directive is very broad and would probably cover the political violence which we think is properly the concern of the security intelligence agency, but it might also be interpreted to cover a great deal more, much of which we think should not be within the security agency's mandate. That paragraph reads as follows:

> (vi) the use or the encouragement of the use of force, violence or any criminal means, or the creation or exploitation of civil disorder, for the purpose of accomplishing any of the activities referred to above;

Earlier when we traced the development of the 1975 Cabinet Directive, we pointed out that this clause was added as a 'basket clause' to the list of activities which constituted the definition of subversive activity in section 16(3) of the Official Secrets Act. Its purpose was to enable the Security Service to continue the full range of surveillance activities which it was then conducting, a number of which, as we shall contend in section B of this chapter, are outside the proper ambit of a security intelligence activity. We think that it is a serious mistake to include any 'basket' clause in the definition of the security intelligence agency's mandate: clauses should not be designed primarily for the purpose of accommodating the Security Service's present range of activity. The general terms of the statutory mandate must be chosen as carefully as possible to reflect what, as a matter of principle, Parliament believes should be regarded as activity threatening the security of Canada.

37. The one phrase in paragraph (vi) which appears to have been the most significant addition to the activities covered by paragraphs (i) to (v) is "the creation or exploitation of civil disorder". While we agree that deliberate attempts to turn peaceful demonstrations into violent confrontations for the purpose of destroying the democratic process of government should be the concern of the security intelligence agency, at the same time we think it is dangerous to include in the mandate of the security intelligence agency any words which might suggest it is authorized to collect intelligence about any organization whose activities might lead to "civil disorder". Here we part company with the Australian Security Intelligence Organization Act of 1979 which includes in its definition of domestic subversion the following:

> (i) activities directed to promoting violence or hatred between different groups of persons in the Australian community so as to endanger the peace, order or good government of the Commonwealth;

In our view, dealing with disorderly assemblies and communal violence is primarily a police responsibility. A mandate to investigate political activity which may lead to civil disorder could justify spying on groups whose radical or

dissenting views may provoke opposing demonstrations. Surveillance of such activity by the state's security agency may seriously interfere with the right to criticize the government or the established social, political and economic order, a right which, so long as it is exercised legally, is basic to the form of democracy we value in Canada. Individuals and groups should not be spied upon or have security files kept on them solely because they plan or participate in political demonstrations to protest government policies or criticize other groups in the community. If the security intelligence agency has reason to suspect some persons taking part in such events of being secret agents of foreign powers or persons who might try to turn a peaceful demonstration into a violent confrontation in order to discredit the democratic process, it should inform the appropriate government officials or the police force whose responsibility it is to maintain the peace at such demonstrations.

38. The activities under the heading of political violence and terrorism about which the security agency should gather intelligence are those directed towards the use or threat of serious acts of violence against persons or property for the purpose of achieving a political objective in Canada or in a foreign country. We emphasize that it is only if the violent acts threatened or carried out are serious that they should be the concern of the security intelligence agency. The objective of security must always be kept in view: the security of the democratic process. We regard activities directed toward political violence as being serious only when they are significant enough to constitute a threat to the effective functioning of the democratic process. Only such activities justify surveillance by a security intelligence agency.

Revolutionary subversion

39. In the preceding paragraphs we dealt with foreign and domestic terrorism and other serious acts or threats of violence directed towards accomplishing political objectives. There is one other category of political activity which could be said to constitute a distinct threat to the security of Canada and should be specifically provided for in the security intelligence agency's mandate. That is the activity of political parties and movements which subscribe to ideologies advocating the ultimate overthrow of the liberal democratic system of government but may not actually be involved in political violence. We refer to the activities of such groups as "revolutionary subversion" for their basic aim goes far beyond the influencing of a particular government policy to the eventual replacing of our system of liberal democratic government by an authoritarian government of the extreme right or left. Such subversion, if successful, would truly be revolutionary.

40. Fortunately, throughout Canada's history such revolutionary movements have not posed a serious threat to Canadian democracy. The principal defence against their growth has been the good judgment of the Canadian electorate. With reference to one of these movements, in 1953, Mr. Justice Ivan Rand of the Supreme Court of Canada, in upholding the right of Communists to serve on the executive of labour unions held that one of the basic considerations shaping legislative policy in Canada was that

> The dangers from the propagation of the Communist dogma lie essentially in the receptivity of the environment. The Canadian social order rests on the enlightened opinion and the reasonable satisfaction of the wants and desires of the people as a whole...[6]

We agree with the philosophy expressed in this dictum. So long as political organizations which espouse totalitarian ideologies stick to the methods of liberal democracy to promote their cause, they should not, simply by virtue of their beliefs, be subject to intrusive investigations by the security intelligence agency. However, through its security intelligence organization the government should be able, by the use of non-intrusive techniques, to keep track of the growth of such movements and understand the impact they are having on Canadian democracy. On the other hand, we must stress that if there is reason to believe that such an organization is involved in activities leading to espionage, sabotage, foreign interference, terrorism or serious political violence, then it should be subject to more intrusive investigation by the security agency.

41. Paragraphs (iii) and (vi) of the 1975 Cabinet Directive cover, among many other things, political activity which is directed towards the ultimate overthrow of liberal democratic government in Canada. But we think this category of revolutionary subversion should be designated as a distinct category of activity in the statutory mandate of the security intelligence agency. Bearing in mind what we say in the preceding paragraph, individuals or groups whose activities fall only under this category should not be subject to intrusive investigations by the security intelligence agency.

WE RECOMMEND THAT legislation establishing Canada's security intelligence agency designate the general categories of activity constituting threats to the security of Canada in relation to which the security intelligence agency is authorized to collect, analyze and report intelligence.

(1)

WE RECOMMEND THAT the categories of activity to be so designated be as follows:

- **(a) activities directed to or in support of the commission of acts of espionage or sabotage (espionage and sabotage to be given the meaning of the offences defined in sections 46(2)(b) and 52 of the Criminal Code and section 3 of the Official Secrets Act);**
- **(b) foreign interference, meaning clandestine or deceptive action taken by or on behalf of any foreign (including Commonwealth) power in Canada to promote the interests of a foreign power;**
- **(c) political violence and terrorism, meaning activities in Canada directed towards or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political objective in Canada or in a foreign country;**
- **(d) revolutionary subversion, meaning activities directed towards or intended ultimately to lead to the destruction or overthrow of the democratic system of government in Canada.**

(2)

[6] *Smith and Rhuland Ltd.* v. *The Queen* [1953] 2 S.C.R. 99.

WE RECOMMEND THAT, for category (d), revolutionary subversion, only non-intrusive techniques be used to collect information about individuals or groups whose known and suspected activities are confined to this category.

(3)

42. We recognize that the definitions of statutory boundaries of security intelligence activities proposed above are cast in very general terms. The meaning which these terms have in practice will depend in large measure on how they are interpreted by members of the security intelligence agency's senior management, government officials and Ministers. That is why we shall lay great emphasis on the quality of the personnel who lead the security agency and carry out its responsibilities. The members of the agency must not see the general statutory definitions of the agency's mandate as something that may be stretched to cover what they personally believe are threats to Canada's security. They must understand and accept the purpose for which the statutory definition is designed. The statutory definitions must also serve as the framework for government direction and review of the agency's functioning.

The need for a limiting clause

43. In addition to positive statutory standards to define what the security intelligence agency may do, we think it would be wise to include in the statute establishing the security intelligence agency a clause indicating what it clearly must not do. For example, section 4(2)(b) of the Act governing New Zealand's Security Intelligence Service states that it shall not be a function of the Security Intelligence Service

> To institute surveillance of any person or class of persons by reason only of his or their involvement in lawful protest or dissent.[7]

The Directive issued by the Secretary of State for the Home Department (Sir David Maxwell Fyfe) in 1952 to the Director General of the Security Service, which remains to this day the fundamental public statement on the role of Britain's security intelligence organization, contains clauses designed to restrict the Security Service's work to what is necessary for the purposes of national security. The Directive first defines the Security Service's purpose in the following terms:

> 2. The Security Service is part of the Defence Forces of the country. Its task is the Defence of the Realm as a whole, from external and internal dangers arising from attempts at espionage and sabotage, or from actions of persons and organizations whether directed from within or without the country, which may be judged to be subversive of the State.

It then adds these limiting clauses:

> 3. You will take special care to see that the work of the Security Service is strictly limited to what is necessary for the purpose of this task.
>
> 4. It is essential that the Security Service should be kept absolutely free from any political bias or influence and nothing should be done that might lend colour to any suggestion that it is concerned with the

[7] New Zealand Security Intelligence Service Amendment Act (1977), s.4(2)(b).

interests of any particular section of the community, or with any other matter than the Defence of the Realm as a whole.

5. No enquiry is to be carried out on behalf of any government department unless you are satisfied that an important interest bearing on the Defence of the Realm, as defined in paragraph 2, is at stake.[8]

44. Nowhere in the various strands of authority to which the R.C.M.P. Security Service looks for a definition of its functions is there any statement of the need to limit security intelligence investigations to what is strictly necessary for the security of Canada. The 1975 Cabinet Directive does not contain any statement which may be interpreted as providing a brake or rein on security intelligence activities. Director General Dare's letter of May 22, 1975, explaining the significance of the Cabinet Directive to senior officers of the Security Service emphasized the expansive nature of the Cabinet's mandate and the lack of constraint, as in the following passage:

> Being granted a broad intelligence base and not being constrained by either ideological or criminal considerations alone, we are now free to respond to current and rapidly changing factors affecting National Security.
>
> (Vol. 141, pp. 21761-63; Ex. M-135.)

Nowhere in the letter is there a reminder to senior officers that there is need for constraint in the exercise of the powers conferred.

45. At the beginning of this part of our Report, in defining the fundamental principles on which Canada's security system should be based, we emphasized the need to ensure that the requirements of security are compatible with the requirements of democracy. Both the government which directs the security agency and the agency itself must constantly keep this fundamental precept in mind. As Rebecca West wrote:

> . . . if we do not keep before us the necessity for uniting care for security with determination to preserve our liberties, we may lose our cause because we have fought too hard. Our task is equivalent to walking on a tightrope over an abyss.[9]

We think a statutory clause stating the need to restrict the security intelligence activities to what is strictly necessary for the security of Canada would make it more likely that those who direct and carry out security work will keep in mind the danger to liberty which can result from an overly expansive interpretation of the security intelligence agency's mandate. Such a clause should combine at least one part of the British Home Secretary's Directive with the restriction contained in the New Zealand Security Intelligence Service Act.

> **WE RECOMMEND THAT the legislation establishing Canada's security intelligence agency contain a clause indicating that the agency's work should be limited to what is strictly necessary for the purpose of protecting the security of Canada and that the security intelligence agency should not investigate any person or group solely on the basis of that person's or group's participation in lawful advocacy, protest or dissent.**
>
> (4)

[8] Quoted in Cmnd 2152, paragraph 238.

[9] Rebecca West, *The New Meaning of Treason*, New York, Compass Books, 1964, p. 370.

The need for coherence and consistency

46. The tasks assigned by government to a security intelligence agency must not require it to collect intelligence on matters which are outside its statutory mandate. As we showed in Part II, Chapter 2, government direction of the security intelligence agency in the past lacked consistency and coherence in this regard. A particularly glaring example of inconsistency, which we outlined in that chapter, was the incompatibility between the instructions given with regard to reporting on "separatist sympathies, associations, and activities" in Public Service Security Screening[10] and the mandate given in the Cabinet Directive of March 27, 1975.

47. In Part VII of this Report, which deals with the security screening work of the security intelligence agency, we shall review the criteria on which decisions to grant security clearances are based. These criteria might be more specific or limited than the general categories which define the statutory limit of security intelligence, but they must not be wider than these definitions nor refer to subjects which cannot be brought under these definitions. Similarly it will be essential to ensure that the definitions of subversive activity or the security of Canada, in legislation such as section 16 of the Official Secrets Act providing special powers (or exemptions) for security purposes, are consistent with the definition of threats to the security of Canada in legislation establishing the security intelligence agency.

WE RECOMMEND THAT all intelligence collection tasks assigned to the security intelligence agency by the government be consistent with the statutory definition of the security intelligence agency's mandate and that all legislation and regulations providing special powers or exemptions for security purposes be consistent with the definition of threats to the security of Canada in the legislation establishing the security intelligence agency.

(5)

The need for flexibility

48. The definitions we have proposed for the security intelligence agency's statutory mandate are cast in quite general terms and should, we think, cover all the specific activities in relation to which Canada may in the foreseeable future require security intelligence. Still, it may be argued that there may be types of activity which we have not anticipated which might pose a serious threat to Canada's security in the future but which would be outside the statutory mandate of the security intelligence agency and outside the scope of criminal investigation agencies. If some new threat to the security of Canada developed which appeared to fall outside the statutory mandate, but which the government believed urgently required investigation by the security agency, there might be difficulty in obtaining quickly enough the statutory amendment needed to provide authorization for the surveillance. There is the danger that the public addition of words to cover the new situation would expose the interest of the agency in the proposed target. Even though we may find it impossible now to give an example of such an eventuality, should the scope of

[10] Paraphrased in Vol. 160, p. 24427. See Ex. M-135.

our national security legislation be bound by our limited knowledge of the future? Or should we avoid trying to legislate for what is presently inconceivable and leave it to future generations of legislators to modify Parliament's identification of the classes of activity about which Canada requires security intelligence?

49. We have concluded that, on balance, it would be best to include an emergency provision in the security intelligence agency's statutory mandate empowering the government by Order-in-Council to extend the security intelligence agency's mandate to an activity which in the government's view constitutes a serious threat to the security of Canada but which is not included in the general categories of activity listed in the agency's statutory mandate. If the statute contains a provision of this kind it should require that the Special Parliamentary Committee on Security and Intelligence be notified on a confidential basis when the Order-in-Council is passed and that within 60 days of its passage such an Order require for its continuation approval by an affirmative resolution of both Houses of Parliament.

WE RECOMMEND THAT there be a provision to extend by Order-in-Council in emergency circumstances the mandate of the security intelligence agency to a category of activity not included in the agency's statutory mandate, providing that the Joint Parliamentary Committee on Security and Intelligence is notified on a confidential basis when the Order-in-Council is passed and that within 60 days of its passage the Order-in-Council is approved by an affirmative resolution of both Houses of Parliament.

(6)

B. DISTINGUISHING DISSENT FROM SUBVERSION: LESSONS FROM THE PAST

50. In the remaining sections of this chapter we review some of the policies and practices which have governed the counter-subversive activities of the R.C.M.P. Security Service. In the decades since World War II, and especially in the 1960s and early 1970s, Security Service surveillance of domestic 'subversion' expanded considerably. Often individuals and groups were investigated who were not involved in espionage, foreign interference or terrorism, or any form of political violence. It is in this area of domestic subversion that improper targetting is most likely to encroach on legitimate dissent. Our objective in reviewing this past activity of the Security Service as part of our proposed Plan For the Future is not primarily to judge past policies — although some judgments must be made — but rather to learn from them and to indicate how these controversial areas would be treated under our recommendations concerning the proper scope of security intelligence surveillance. In keeping with this objective, we shall make no further recommendations in this chapter. Where recommendations appear to be called for, they will be included in a more complete discussion in other parts of our Report.

51. The most important lesson to emerge from a review of counter-subversion activities is that security intelligence activities must be subject to well-defined,

clearly communicated government policies. In the past the Security Service was left without guidance or else was given too much discretion in determining appropriate targets or subjects of investigation. In large part, the lack of a clear legislative mandate and of continuing supervision by government of security intelligence activities left the Service on its own to make important policy decisions often involving sophisticated political judgment. At times, either through misinterpreting the position of government or perhaps just acting cautiously, the Security Service failed to respond adequately to Canada's security needs; at other times we think there was an excess of zeal.

52. When Cabinet did give attention to security matters, as with R.C.M.P. operations on university campuses and the coverage of separatism in Quebec, its directives were not always clear, or else were not accurately transmitted by the Security Service to members in the field. Throughout, there have been problems of communication between the Security Service and government, heightened no doubt by the need for secrecy and by the lack of formal and effective institutions of supervision and control. Much has depended on the close but uncertain relationships between senior officers of the Security Service and various Commissioners of the R.C.M.P., senior civil servants and Ministers. The result has been that in determining broad operational policy the Security Service has often taken its own counsel and functioned in isolation from the other organs of government.

53. There will always be isolation in security work. To the limited extent that investigators and analysts talk about their work they do so only with colleagues in the security community. Their perceptions are therefore likely to become somewhat conformist and cautious. This makes it all the more important in a free society for major policy decisions on investigations to be made with the full and active involvement of Ministers and senior officials. But as some of the cases that we review in this chapter illustrate, the involvement of Ministers and senior officials is not enough to ensure legal and proper behaviour in an area of government shrouded in secrecy. Thus, we shall recommend in later chapters of this Report the establishment of a parliamentary committee and an independent review agency to scrutinize security intelligence activities. In addition, we shall propose the involvement of the judiciary in authorizing the use of certain particularly intrusive investigative techniques.

54. In reviewing the past we readily acknowledge the benefits of hindsight. Second guessing is far easier than making decisions on complex matters, especially when such decisions are made under great time pressures with little or no direction from government. We should also note that we are examining policies developed for the most part in the 1960s and early 1970s. This was a period of some turbulence in Canada in contrast to the present, which, from a security perspective, is a relatively placid time in our history. This marked change in the level of social conflict adds to the difficulties of being fair and balanced in our assessment of the past.

55. Another factor to keep in mind when reading this chapter is that these events were not unique to Canada. Book III of the *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence*

Activities[11] (commonly referred to as the Church Committee's Report) contains close to 1000 pages of evidence of questionable activities of the FBI, CIA, and other United States intelligence agencies in the area of counter-subversion during the 1960s and early 1970s. Acting Justice White's report on *Special Branch Security Records*[12] completed in 1977 in the State of South Australia also covers topics similar to those dealt with in this chapter. While the activities of security agencies in other liberal democracies are, with few exceptions, not a matter of public record, we would be surprised if these countries were completely immune from the kind of excesses recorded in this chapter. That at least some of the Security Service's sister agencies were engaged in similar activities does not excuse what happened in Canada, but it does increase our understanding of why improprieties and illegalities occurred. In the secret and closely knit world of security intelligence, the perspectives and activities of sister agencies must have had some influence on the Security Service, especially in a situation where little direction was forthcoming from government.

56. We are under no illusions about the ease of drawing a clear line between dissent and subversion. For those responsible for making targetting decisions about domestic groups and individuals, the task is akin to distinguishing between subtle shadings of grey. There are few 'blacks' and 'whites' in this business. Thus, while it is appropriate for a security intelligence agency to investigate individuals suspected of planning political violence, or acts of foreign interference, it is not nearly so obvious what the agency should do in the case of individuals who merely advocate the use of violence. Moreover, once an investigation is launched, there is the question of how the investigation should proceed with regard to the legitimate organizations to which the individual under investigation belongs. Given the difficult and continuing nature of this dilemma, we believe that those within the security intelligence agency must exhibit great care and sensitivity in making targetting decisions, that others outside the agency, including Ministers, should be involved in these decisions, and that there be some mechanism for *ex post facto* review so that the agency and the government will continually learn from the past.

57. Having made these preliminary observations let us turn to the lessons of the past. We shall discuss a number of topics which relate to surveillance policies regarding domestic subversion: separatism and national unity, surveillance on university campuses, the Extra Parliamentary Opposition, political parties, labour unions, blacks, Indians and right wing groups. It must be emphasized that these subjects do not constitute a comprehensive description, or even a profile, of the work of the Security Service. There has been no attempt to provide examples of counter-espionage, international terrorism or the surveillance of Communist or other groups whose avowed objective is the

[11] U.S. Senate, *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, Book III, U.S. Government Printing Office, Washington, 1976.

[12] *Special Branch Security Records*, an Initial Report to the Premier of South Australia, Mr. Acting Justice White, Adelaide, 1977.

ultimate overthrow of our democratic system. Generally speaking, the Security Service experienced fewer difficulties in understanding and implementing its role in connection with espionage, foreign interference and international terrorism.

58. In discussing these topics, we shall tend to treat them as if they were in distinct pigeonholes. Of course, some subjects are unrelated. However, in the early '70s the Security Service's perception that Communists and Marxists were adopting new techniques, outside the Communist Party, to infiltrate a variety of institutions (including governments, universities, ethnic movements and a political party) resulted in a concerted effort to investigate the extent of such penetration of "key sectors" of society. Impetus for this development also came from the rising tide of student violence in this country, the United States and Europe, and the emergence of philosophies that preached violent assault on the established order. In 1970 the Director General of the Security Service predicted (wrongly, as it turned out) a decade of increasing disorder, and so advised the government. Consequently, throughout Canada — and totally unrelated to the separatist concern — the Security Service perceived the future as requiring an intensified level of investigation in order that government and police forces would not be caught unawares in the event of serious outbreaks of violence for political purposes. The Security Service terminated the "key sectors" programme in 1977 after a long internal review of the value of the programme.

(a) *Separatism and national unity*

59. Since the early 1960s one of the most difficult policy questions relating to the R.C.M.P. Security Service has been the proper definition of its role with respect to Quebec separatism and the national unity issue. It is an urgent question for Canadian democracy and Canadian security and it is still unanswered. Too broad a role can endanger Canadian democracy by undermining constitutional methods of settling the future of the Canadian federation. A role which is too narrow can deprive the federal government, as well as provincial governments and local police forces, of timely and useful intelligence about threats of *violent* political action.

60. The record of policy-making on this issue reveals a great deal of vagueness, confusion and ambiguity in both government direction and the Security Service's response to that direction. The story of the R.C.M.P.'s role in this area provides one of the best illustrations of the need for a clear definition of the role of the security intelligence agency — one which is understood and accepted by Parliament and the Canadian people.

61. The historical record can be divided into four distinct periods:

1. 1963-67: when the focus of R.C.M.P. security intelligence collection was strictly on terrorist elements in the separatist movement.
2. 1967-75: when R.C.M.P. security intelligence collection activities expanded to include open and democratic separatist parties and groups.
3. 1975-76: when confusion resulted from conflicting government directions on general surveillance and security screening.

4. 1976-78: when there were efforts to clarify or redefine the Security Service's role with respect to separatism.

62. In examining this historical record our focus is exclusively on policy rather than on actual operations in the field. A later Report will contain our findings as to some R.C.M.P. practices not authorized or provided for by law in gathering intelligence about and countering separatism in Quebec. The basic policy question of concern to us here is the extent to which separatism and any other attempts to bring about fundamental changes in Canada's Constitution have been, and ought to be, subject to the surveillance of a security intelligence agency.

1963-67: focus on terrorism

63. In the early and mid-1960s the Security Service understood that its basic role in relation to separatism was to collect information about separatists who used violent or terrorist methods to gain their ends. Assistant Commissioner Bordeleau, the Director of Security and Intelligence, writing to the officer in charge of the Quebec Division in October, 1963, explained that:

> It is fundamental in defining the extent of our interest in the movement to accept that there is nothing intrinsically illegal about it (i.e. separatism), nor should the "separatists", "independentists" etc. come under police investigation provided they confine themselves to constitutional methods.

64. F.L.Q. bombings were beginning to occur. The R.C.M.P.'s main security intelligence task was to penetrate the terrorist elements of the separatist movement. Assistant Commissioner Bordeleau said that the biggest obstacle in performing this task was that "most F.L.Q. activities were taking place amongst university students and teachers, who are presently practically immune from investigation". This understanding of government policy with regard to university surveillance differed from that of certain Ministers and their officials. Moreover, the R.C.M.P. made little effort to have changed what it believed to be an overly restrictive policy. As a result, there may have been a failure to carry out investigations of F.L.Q. terrorism — investigations which might have prevented some of the serious terrorist attacks before and during 1970. This episode is an indication of how the security of Canada may suffer when communications between a security intelligence agency and the rest of government are poor. (We discuss the question of investigations at educational institutions in more detail later in this chapter.)

65. The only other policy problem which arose during this period was that of providing security clearance reports on government employees who were members of open, legal, democratic separatist groups. Departments were beginning to request such information about employees and applicants. The Security Panel had a lengthy discussion of this matter on September 23, 1964. There was some support at that meeting for confining screening reports to information about participation in separatist activities of an illegal and terrorist nature. But the view prevailed, according to the minutes of the meeting, that the R.C.M.P. should include in their reports to Departments the fact of membership in open separatist organizations together with the "detailed information concerning length of attendance, the degree of involvement, and

other pertinent information as was available". Also according to the minutes, the decision of that Panel was to be referred to the Cabinet Committee on Security and Intelligence for its consideration. We have found no record of Cabinet Committee consideration of this matter, except several years later.

66. The Security Panel's decision raises a crucial question which was not discussed at its meeting: *how* was information about membership, degree of involvement and other aspects of open separatist organizations to be 'available' to the R.C.M.P.? Failure to face this question created ambiguity as to the Security and Intelligence Directorate's role in *collecting* intelligence about open separatist organizations. Was it to begin collecting information by reading the newspapers or by developing sources? Was it simply to sit back and wait for someone to drop relevant information into its lap? When intelligence agencies are told by senior members of the government to report certain information "if it is available", there is a danger that they will treat such direction as an instruction to collect as well as to report.

67. In any event, the security screening branch of the Security and Intelligence Directorate began reporting "separatist information" to Departments in April 1965. The R.C.M.P. and the Assistant Secretary to the Cabinet for Security worked out an arrangement whereby information was to be reported if it fell into one of the following three categories:

(1) subject or a relative of the subject participates in or is connected with "separatist/terrorist activities or movement"

(2) subject is an active participant or member of a Separatist movement

(3) subject has a relative who is an executive member of a Separatist movement.

Some of the people who would come within these categories — namely, those whose only separatist activity was of the open, democratic kind — clearly did not fall within the categories of persons set out in the Cabinet Directive governing security screening.[13] Thus the Security Panel's direction, the vagueness of which was graphically symbolized by the use of an ambiguous oblique in the phrase "separatist/terrorist activities", and the R.C.M.P.'s response to it, raise the question of whether the Force was involved in the reporting (and possibly the collection) of information in areas not authorized by the Cabinet. (We have discussed this matter in Part III, Chapter 11.)

1967-75: expansive coverage of separatism

68. In 1967 there was a decisive change in the federal government's perception of the separatist threat. It was now not only a security threat, it was a serious political threat. The federal government was concerned not only about threats of political violence but also with the political support the separatist movement was attracting from the Quebec electorate. Politicians and officials involved in government decision-making naturally and quite properly should be

[13] See Part VII, Chapter 1 for that section of Cabinet Directive 35 which sets out the categories of persons who are to be denied a security clearance on "disloyalty" grounds.

concerned with both the political and security dimensions of a political movement as important as Quebec separatism, but it is quite another matter to use a security intelligence agency to gather information about not only its security dimensions but its political dimensions. The central characteristic of this period is a vague intermingling of political and security concerns in government direction of the Security Service, and, not surprisingly, in the Security Service's response to that direction.

69. On August 14, 1967, at Prime Minister Pearson's direction, the Security Panel met to discuss ways and means of increasing the intelligence on separatism available to the government. According to Deputy Commissioner Kelly's record of this meeting, separatism was identified as a greater danger than Communist activities. Three overlapping concerns were identified: terrorists, constitutional separatism and foreign involvement. Mr. Kelly reported that "the general tone" of the meeting indicated that the R.C.M.P. were expected at this time to know more than it did about what was going on in the Province of Quebec in relation to Separatism.

70. This meeting was a critical turning point in the broadening of the R.C.M.P.'s security intelligence coverage of separatism. In his testimony Mr. Starnes stated that:

> ... there is no doubt that if the government had not wished to have separatism dealt with by the Security Service in the way in which they dealt with it, there is no question that the Security Service would not have done it, in its wildest dreams, there is no way the Security Service on its own would undertake that kind of investigation.
>
> (Vol. 100, p. 15938.)

Mr. Starnes admitted that the government never made "any declaration that the separatist movement was subversive" (Vol. 100, pp. 15935-6). Still he insisted that the Security Service had a broad mandate from government to investigate separatism as a whole, not simply its terrorist or violent elements, and traced that mandate back to "when they first started their discussions of this matter... in 1967, and the continuum from that time through to the early '70s was quite clear and it is established" (Vol. 100, p. 15939).

71. The government's vague broadening of the R.C.M.P.'s mandate for collecting information about separatism caused senior R.C.M.P. officers to be extremely concerned about the political consequences such a broadening might have for the Force. This concern is clearly reflected in the records of meetings held within the R.C.M.P. in August 1967. Security intelligence officers in the R.C.M.P. regarded such an expanded mandate as outside the role of a "defensive service". Intelligence requirements would, among other things, require forms of surveillance within Canada and the collection of intelligence outside Canada which, they thought, would be work appropriate to an offensive intelligence agency. These senior R.C.M.P. officers were very worried about the political consequences if surveillance of this kind were publicly exposed and considered that the Force should not enter into this new area without new terms of reference. There was some discussion of the merits of setting up a separate agency under Privy Council Office auspices for this intelligence task,

so that the R.C.M.P. would not bear the brunt of any potential political criticism.

72. Despite these qualms and the desire for clear government authorization, the R.C.M.P.'s Security and Intelligence Directorate expanded its coverage of Quebec separatism to include "constitutional separatism" and "foreign intervention". This was done without a written authorization from the government. Instructions sent on November 1, 1968, by a senior officer in the Security and Intelligence Directorate to the officer commanding the Quebec and Montreal security intelligence subdivisions indicate the extent to which the R.C.M.P. was endeavouring to expand its surveillance of separatism. These instructions were issued at the time when the Ralliement pour L'indépendence Nationale (R.I.N.) was breaking up and a large segment of it was merging with René Levesque's Mouvement Souveraineté Association to form the Parti Québecois. Intelligence was to be collected within the P.Q. The instructions made it clear that two kinds of information were wanted:

> (a) An *Intelligence interest*: we seek information on the identity, attitudes and potential of executive and other significantly important members of the Parti Québecois as part of an attempt to assess and anticipate potential and future course (sic) of the Party. We are also interested in both open and closed information as to the Party's strategy and tactics, financial condition, membership quantity and quality, relations with other political parties and pressure groups (such as trade unions and media of information) and on any existing or future relationships with foreign countries or subversive groups such as Communist or Trotskyist parties and so on.
>
> (b) A *Police* interest: we must continue to seek to identify and maintain a continuing study of those individuals in the Parti Québecois who advocate subversive or illegal courses of action or who are members of or sympathizers with outside groups which do so.

73. Information of the first type — the "Intelligence Interest" — is clearly information that goes beyond purely security matters and into the realm of politics. The closest the R.C.M.P. seems to have come to obtaining an explicit mandate from the Cabinet for the collection of this type of information was at the meeting of the Cabinet Committee on Security and Intelligence held on December 19, 1969. According to Commissioner Higgitt's notes of that meeting, one of the Committee's recommendations included the following:

> R.C.M.P. asked to provide a detailed report on the present state of separatism in Quebec in terms of organization, numbers involved, organizational inter-relationship, apparent strategy and tactics and outside influence.

74. The blending together of political and security purposes can be seen in subsequent targetting directions issued by the Security Service. In September 1970, when "G" Branch was being established in "C" Division (i.e. the Quebec Division) to focus on Quebec separatism, the Director General, Mr. Starnes, wrote to the officer in command of the security intelligence units in "C" Division, attaching terms of reference for "G" Branch. These terms of reference set out the following objectives for the branch:

To be as fully informed as possible on:

— all Separatist/Terrorist activities in the Province of Quebec

— all activities by foreign powers which may affect the position of Quebec in Confederation

— all activities by subversive organizations which touch on the Quebec problem

— developments of a subversive nature among the French speaking population of other provinces.

The terms of reference went on to give sweeping instructions with regard to separatism:

> In order to obtain adequate information regarding Separatist activities, "G" Branch must develop sources in all organizations and among all persons supporting the separation of Quebec from Canada...
>
> Clearly, the Parti Québecois, because it has attracted so many persons who are prepared to go to great lengths to achieve a separate Quebec, must be regarded as a prime target. Investigation of the P.Q., of course, has as its main purpose the achievements of a better insight into those activities within the party which clearly are subversive and have as their aim the break-up of confederation. In particular "G" Branch should build up an intimate knowledge of the party, its structure, its finances, its aims and those responsible for its direction. Among other things such knowledge is necessary in order to identify those elements in the party who may attempt to subvert it to the achievement of a separate Quebec by any means, including the use of force and terroristic acts. In addition the Branch should develop information regarding individuals or groups of individuals within other political parties who seek a separate Quebec by any means.

Mr. Starnes' covering letter stated that "the resources available to us in "C" Division will have to be utilized to the full if the government's priority of maintaining national unity is to be aggressively pursued."

75. The instructions quoted above show how easy it was at this time for members of the Security Service, including Mr. Starnes, to consider that any attempts to "break up Confederation" by democratic or any other means constituted a security threat warranting surveillance and investigation by the R.C.M.P.'s security intelligence branch. In his testimony, Mr. Starnes said that the Prime Minister congratulated him on a brief he had prepared in 1970 for the Interdepartmental Committee on Law and Order analyzing Separatist activities — a brief which included a section on the Parti Québecois. He testified that:

> ... we were not targetting the Parti Québecois as such, and we were very careful not to do so.
>
> But we were concerned with some of the elements which are described in the Royal Commission Report, which would be: foreign involvement, subversive activities, terrorist activities, infiltration of the Parti Québecois by some of the elements.
>
> (Vol. 100, pp. 15951-2.)

His testimony that there was a narrow focus and purpose of Security Service surveillance of the P.Q., limited strictly to concerns of security, is difficult to

reconcile with the broad references to political concerns about the future of Confederation found in his instructions to "G" Branch, quoted above. Nor is it easy to reconcile his testimony with the activities of the Security Service throughout most of the 1970s in collecting intelligence about the Quebec Liberal Government and the Parti Québecois.

76. Two further developments in the early 1970s accentuated the tendency to merge political and security interests in the Security Service's coverage of separatism. The first was a decision made by the Security Advisory Committee in 1972 which, in effect, formalized the arrangement made nearly eight years earlier with respect to reporting separatist information for security clearance purposes. At a meeting on November 14, 1972, the Committee noted that with respect to "information relating to separatism":

> neither Cabinet Directive 35 nor the security policy statements made by Prime Minister Pearson and Justice Minister Chevrier in 1963 provided authority for Security Service reporting of information in this area, in relation to screening public servants.

The Committee took cognizance of the fact that despite the lack of explicit Cabinet authorization the Security Service had been reporting information on a person's involvement in the separatist movement directly to the Privy Council Office, which would in turn consult with the Departments on the weight to be given such information in the security clearance process.

77. A month later, the Security Advisory Committee resolved this matter, at least to its own satisfaction. The Security Service was now to report information on a person's links with separatism directly to departments. But the Privy Council Office was to be consulted before any decision was taken to deny clearance on the basis of such information. The scope of Security Service information on separatist links was defined as follows:

> Separatist sympathies, associations and activities on the part of the subject will be reported as will significant separatist information on relatives and associates.[14]

This decision was circulated to Deputy Ministers and heads of agencies on December 15, 1972 in a memorandum signed by the Secretary to the Security Advisory Committee. There is no indication that it was considered by the Interdepartmental or Cabinet Committees on Security and Intelligence. Once again there is no indication that the implications of this decision for the R.C.M.P. Security Service's programme of *collecting* information were considered. Again there was no conscious recognition of the connection between government direction to report information and a security intelligence agency's mandate to collect it.

78. The second development occurred late in 1974, when the Security Service re-adjusted and clarified its policy with regard to surveillance of the Parti Québecois. This reconsideration was prompted by the emergence of the P.Q. as a major political party in the Province of Quebec and a serious contender for

[14] All but the last nine words of this sentence were discussed in evidence publicly: Vol. 141, p. 21672.

power. Thus Security Service targetting of the P.Q. now entailed surveillance and investigation of a democratic political party which was in the mainstream of provincial politics and might in the foreseeable future win an election and form a provincial government. The political implications of targetting, which had always worried the Force, were now more apparent than ever. Nonetheless, the new policy adopted by the Security Service called for sufficient surveillance of the P.Q. to determine how influential it was becoming in key sectors of Quebec society and whether or not the Party was receiving assistance from foreign countries. Thus, this new policy explicitly rejected the recommendation of the Royal Commission on Security whose recommendation on security intelligence surveillance of separatists had been as follows:

> Separatism in Quebec, if it commits no illegalities and appears to seek its ends by legal and democratic means, must be regarded as a political movement, to be dealt with in a political rather than a security context. However, if there is any evidence of an intention to engage in subversive or seditious activities, or if there is any suggestion of foreign influence, it seems to us inescapable that the federal government has a clear duty to take such security measures as are necessary to protect the integrity of the federation. At the very least it must take adequate steps to inform itself of any such threats, and to collect full information about the intentions and capabilities of individuals or movements whose object is to destroy the federation by subversive or seditious methods.[15]

The rationale for security surveillance of the Parti Québecois was based on the P.Q.'s objective of breaking up the Canadian federation; the Security Service decided that it should analyze "the forces actively working at destroying the unity of the country", so that the Security Service could become "a meaningful depository of this data which the Government could rely upon before taking decisions affecting national unity". This policy was approved by the Director General, Mr. Dare, on June 3, 1974. The operational implications of the policy were summarized in an internal Security Service memorandum as follows:

— No coverage of electoral activities.

— No collecting of membership lists.

— Selective clippings only.

— Minimal investigation of financial resources.

— Monthly analytical review of:

(a) Influence of newspaper "Le Jour".

(b) P.Q./labour unions relationship.

(c) P.Q. activities within politicized pressure groups.

— Investigate leads of foreign interference tied in with P.Q.

— Isolate radical elements operating under P.Q. cover.

— Investigate leaks of privileged information belonging to federal government.

— Tightening of security concerning the reporting of investigations of P.Q. activities.

[15] *Report of Royal Commission on Security*, 1969, para. 21.

— No discussion of our policy on P.Q. with Q.P.F. and S.P.C.U.M. [i.e. with the Quebec Provincial Police and the Montreal Urban Community Police Force].

— Initiation of discussion with P.S.P.B. [i.e. Police and Security Policy Branch in Solicitor General's Department] to formalize above mentioned coverage.

79. It is important to note that Mr. Dare approved all of these recommendations except the proposal to discuss the matter with the Solicitor General's Department. The Director General gave the following reasons for not seeking explicit approval for this policy from the Minister:

> Firstly, the information gathered will be made available to the government by a report to the Minister as required from time to time. Secondly, the Prime Minister has expressed to me and my predecessor his concern regarding separatism and I have the responsibility to report to both he [sic] and the Minister any major events or trends. We must all realize that the unity of our country is vital to the federal government.

80. Thus this period ends with the adoption of a formal policy by the Security Service on its coverage of separatism in Quebec. Apparently this policy was not submitted for approval to the Minister responsible for the Security Service nor to the Cabinet. It was a policy which in effect rejected the recommendations of the Royal Commission on Security. Finally, it was a policy which did not differentiate between the political and the security aspects of the P.Q. or of separatism. Indeed the tone of the policy statement and Mr. Dare's letter of approval indicate how difficult it was for members of the Security Service and, indeed, senior officials and Ministers, to adopt the approach recommended by the Royal Commission and to differentiate between the political and security implications of Quebec separatism.

1975-76: attempts to develop policy

81. In 1975 the government, at the Cabinet level, finally began to make policy with regard to the Security Service surveillance of the P.Q. and separatism. But policy was developed and enunciated in a manner which resulted in great confusion for the R.C.M.P.'s Security Service and for the public, and perhaps even for the policy-makers themselves. The heart of the confusion was and is the relationship between the direction the government gave the Security Service with respect to investigation of separatism generally, and the direction it had earlier given the Security Service concerning security clearances. Our perception is that at the time the March 1975 mandate was established the government did not consider that relationship and the Security Service did not bring the relationship to the attention of the government. The failure of the Security Service to do so was probably due to its lack of appreciation of the significance of the relationship.

82. The problem began in March 1975, when the Cabinet approved the Security Service's "mandate" in the form of a Cabinet Directive which we discussed in some detail earlier in this chapter. One interpretation of the mandate might be that the authorization given to the Security Service to investigate separatism and the Parti Québecois had been considerably reduced.

Thus, both the wide coverage approved by Mr. Dare in June 1974 and the collection of information about "separatist sympathies, associations and activities" which the Security Panel had formally authorized in 1972, might be precluded by the 1975 mandate. However, it was possible to read the mandate otherwise; there is evidence that the Cabinet may have expected paragraph (f) of the mandate to allow the monitoring of the activities of separatists. This interpretation, which may be justified by Mr. Dare's knowledge of the background of the Cabinet's decision, was stated in the following paragraph of his letter of May 22, 1975, in which he communicated the terms of the Cabinet Directive to all branches of the Security Service.

> In seeking new guidelines, the R.C.M.P. Security Service did not attempt to fundamentally alter our current activities — the collection of intelligence relating to espionage, sabotage, subversion and terrorism — rather we sought to formalize guidelines which Government had already recognized in a general way. Due to the fluid nature of national and international events, we will continue to monitor traditional areas of interest — such as Communists, Trotskyists, Maoists, *separatists*, black revolutionaries, native extremists, right-wing extremists and revolutionaries from other countries resident in Canada — although in many of these areas we may shift from aggressive collection to a passive monitoring role. Being granted a broad intelligence collection base and not being constrained by either ideological or criminal considerations alone, we are now free to respond to current and rapidly changing factors affecting National Security.
>
> (Our emphasis.)

83. However, on June 9, 1975, Mr. Dare wrote to the officers in charge of the Ottawa and Quebec area commands of the Security Service with reference to his earlier approval in June 1974, of policy concerning coverage of separatism in Quebec. In his letter he said:

> Recently I met with the Prime Minister of Canada, Mr. Pierre Elliot [sic] Trudeau, and we discussed the criteria used to investigate the Parti Québecois and its members. The Prime Minister stated that the Security Service of the R.C.M.P. does not have a mandate to conduct these enquiries unless they fall within Items A to F of our Role, Tasks and Methods of the R.C.M.P. Security Service.
>
> Therefore, will you please ensure that all enquiries being conducted on the Parti Québecois and its members cease unless they fall within Items A to F of the Role, Tasks and Methods of the R.C.M.P. Security Service.

As we shall see, nearly a year later, when an opposition member in the House of Commons raised the matter, Mr. Trudeau and Mr. Allmand stated that the "recent meeting" referred to by Mr. Dare had been the March 1975 meeting of the Cabinet Committee on Security and Intelligence when it agreed to the general mandate of the Security Service.

84. On June 13, 1975, Mr. Dare wrote to Mr. Bourne, Chairman of the Security Advisory Committee that the Prime Minister's guidelines "restricting the Security Service's enquiries with regard to the Parti Québecois" may conflict with the 1972 Security Panel's requirement concerning the reporting of information about separatist sympathies, associations and memberships for

security screening purposes. He asked that the Security Advisory Committee consider this matter at its next meeting. Despite at least this one documented attempt, Mr. Dare did not get the matter resolved by the government committees.

85. By February 1, 1976, the Security Service considered that its information on separatists was out of date, and that the Security Service was unable to provide accurate assessments of current activities and was providing incomplete and possibly erroneous assessments and information to departments. Consequently, Mr. Dare wrote to Mr. Bourne to inform him that the Security Service could not be expected to provide the type of information Deputy Ministers and heads of agencies required for security screening purposes. On May 5, 1976, a newspaper article quoted from Mr. Dare's letter of February 1, 1976 under the banner heading: TRUDEAU HALTS SCREENING OF CIVIL SERVICE SEPARATISTS. On May 5, 1976, Mr. Erik Nielsen, M.P., questioned Prime Minister Trudeau in the House of Commons about the leaked letter. The focus of his questions concerned the possible impropriety of the Prime Minister's personally having issued guidelines to the R.C.M.P. Mr. Trudeau replied:

> There were no guidelines issued by me or any interference by me. There is a cabinet committee on security and intelligence which oversees the operation of government agents in the area of security and intelligence. Certain conclusions were reached which were communicated to the police. They were not communicated by me personally or under my name. They were the object of a cabinet decision.[16]

86. The next day the Solicitor General, Mr. Allmand, reported to the House of Commons that what Mr. Dare referred to as guidelines was actually the Cabinet decision (of March 27, 1975) with regard to the mandate of the Security Service. This decision, Mr. Allmand said, was based on a submission he himself had presented to Cabinet and among other things it:

> . . . confirmed that the R.C.M.P. should not survey legitimate political parties per se, but of course individuals in all political parties should be subject to surveillance if they are suspect with regard to criminal activities, subversion, violence or anything like that.

He said that these guidelines dealt with general operations only and not with security screening. He also stated that:

> . . . the decision General Dare was talking about, the cabinet decision, was a decision of the cabinet as a whole and the cabinet committee as a whole and was not the result of any private meeting between General Dare and the Prime Minister.[17]

87. On May 11, 1976, in the House of Commons, Prime Minister Trudeau gave the following explanation of Mr. Dare's mistake in having referred to the Cabinet's general directive as if it had been a personal instruction from the Prime Minister to restrict surveillance of the Parti Québecois:

> The mistake probably arises from the fact that as a member of that cabinet committee, I did of course participate. I do not mind admitting I was one of

[16] House of Commons, *Debates*, May 5, 1976, p. 13193.
[17] *Ibid.*, May 6, 1976, p. 13224.

those who would argue that a democratic political party should not be under systematic surveillance by the RCMP.

Mr. Trudeau went on to explain his general position on Security Service surveillance of political parties:

> My opinion on that, which was expressed in cabinet, is certainly protected by the usage concerning cabinet secrecy, but I do not mind repeating it here. It is my view and the view of the government that if the party is legal, it should not be under surveillance systematically by the Royal Canadian Mounted Police or any other police. I hope that is the view of the other side of the House.

Finally Mr. Trudeau told the House that Mr. Dare was incorrect in drawing an inference regarding security screening from the Cabinet Directive. That mistake he explained was the following:

> This inference, that because the party is not under surveillance the government does not want to have security clearance on everyone who occupies a sensitive position in the federal government, is wrong.[18]

88. Material in R.C.M.P. files confirms that Ministers, during the meeting of the Cabinet Committee on Security and Intelligence on March 20, 1975, did indeed discuss the question of Security Service surveillance of democratic political parties. An excerpt from a memorandum written by Mr. Gordon Robertson, Secretary to the Cabinet, to Prime Minister Trudeau on April 1, 1976 is as follows:

> At a meeting on 20 March, 1975, the Cabinet Committee on Security and Intelligence considered a memorandum of the Solicitor General on the role, tasks and methods of the R.C.M.P. Security Service. The Cabinet Committee agreed to (and the Cabinet confirmed) the Solicitor General's recommendation that the Security Service be authorized to monitor and investigate individuals and groups in Canada when there are reasonable grounds to believe they may be engaged in, or planning to engage in, a number of specified categories of activities, including espionage, sabotage, terrorist acts and change of government by force or violence. The decision was in general terms, and made no reference to the Parti Quebecois or any other specific group and the categories did not include the activities or goals of the Parti Quebecois. However, you may recall that, during the meeting, Ministers discussed at some length the relation between the proposed role of the Security Service and a legal organization which advocated fundamental change (e.g. dissolution of a federation) by peaceful democratic means. There was a general consensus that in such cases, Security Service surveillance should occur only when it seemed justified in the light of the approved categories.

There is contradictory evidence as to whether, in addition, a "private meeting" between Mr. Dare and Mr. Trudeau occurred to discuss this matter. On the one hand, Mr. Dare testified that, when he referred in his letter of June 9, 1975, to a meeting with the Prime Minister, he did not mean that there had been a private meeting between himself and the Prime Minister. Rather, he stated that he received instructions regarding surveillance of the P.Q. at a

[18] *Ibid.*, May 11, 1976, p. 13389.

meeting of officials and ministers, at which the Prime Minister was present. This meeting took place ". . . towards the end of May or very early June", 1975 (Vol. C89, p. 12252). It is not clear from his testimony whether this meeting was "the fringe of a Cabinet meeting", a formal meeting of the Cabinet Committee on Security and Intelligence, or a meeting held just prior to a formal Cabinet Committee meeting (Vol. C89, pp. 12252-53; Vol. C90A, p. 12431 and 12434). On the other hand, Mr. Gordon Robertson testified that he had ". . . no recollection of any Cabinet Committee meeting of the kind that Mr. Dare is apparently referring to" (Vol. C116, p. 15001), nor did he recall ". . . a meeting at which people stayed behind in order to have a subsequent private discussion" (Vol. C116, p. 15003). Rather he was under the impression that ". . . the discussion was in a meeting in the Prime Minister's office and was a private meeting" (Vol. C116, p. 15002).

89. On May 18, 1976, the Cabinet Committee on Security and Intelligence met and agreed upon the security screening implications of the March 27, 1975 Cabinet decision. The Committee's decision was confirmed by the full Cabinet on May 27, 1976. It was as follows:

Security screening: implications of Cabinet decision of March 27, 1975

> The Committee agreed that the Cabinet decision of March 27, 1975 (166-75RD) was not intended to alter the policy of the government with respect to the screening of persons for appointment to sensitive positions in the Public Service, namely that:
>
> (a) information that a candidate for appointment to a sensitive position in the public service, or a person already in such a position, is a separatist or a supporter of the Parti Québecois, is relevant to national security and is to be brought to the attention of the appropriate authorities if it is available; and
>
> (b) the weight to be given to such information will be for consideration by such authorities, taking into account all relevant circumstances, including the sources and apparent authenticity of the information and the sensitivity of the position.[19]

The Cabinet Committee did not explain how information about a person's separatist leanings or associations was to be available if the Security Service could not systematically collect such information.

90. As a result, on February 8, 1977, instructions were sent by Security Service Headquarters to the officers in charge of the Security Service's Ottawa and Montreal divisions explaining that the Cabinet had directed that inquiries could be made concerning "separatists and supporters of the Parti Québecois". Mr. Dare's testimony gave additional insights into Security Service policy for carrying out these enquiries. For example, he testified as follows regarding field investigations for security screening purposes:

> Q. Would I not be correct that under the directives given ... .that when the inquiry was made of the neighbour one of the questions to be asked would be "Is X a separatist, to your knowledge?"

[19] The contents of paragraph (a) were stated in evidence publicly: Vol. 141, p. 21676.

A. It could well be, Mr. Chairman, yes.

Q. Would a further question also not be "Is X a supporter of the Parti Québecois?"

A. Well, I suppose it could be, Mr. Chairman, but I think we are touching on — yes, it could Mr. Chairman.

(Vol.C90A, p.12383)

Mr. Dare also testified that except for one brief period between February 8, 1977 and April 12, 1977, Security Service policy has been to obtain information about separatism in Quebec for security screening purposes from existing sources and files. Thus, the Security Service appears not to have been cultivating new sources for this purpose (Vol.C90A, pp.12367-12372). According to Mr. Dare, the Security Service, for security clearance purposes regarding separatists, also relied on "spin-off" information — that is information collected accidentally in the course of another investigation (Vol.C-89, p.12278).

91. That is the end of the chronology of a confusing situation. The testimony of Mr. Gordon Robertson, who was the senior government official dealing with security matters from 1963 to 1977 (Vol. C107, pp.13850-1), reveals that this confusion was not the result of the ignorance of Ministers and senior officials about the difficulties that their instructions posed for the Security Service:

Q. So, you were familiar with the dilemma that the Security Service felt in attempting to respond to the government's request for more information about separatists and terrorists and the fact that some of these elements or individuals could be regrouped in a political party which was not subject to or not supposed to be subject to surveillance?

A. Oh, I knew it. I understood it. I had great sympathy with the problem. I think that the Ministers who were connected with it, like the Prime Minister, also understood the terrible difficulty of the problem.

(Vol.C107, p.14057.)

But Mr. Robertson's testimony also reveals that, according to him, instructions to collect information on separatists were premised on a policy established as early as 1964 that "democratic parties" were not subject to surveillance. Consider the following testimony of Mr. Robertson:

Q. The Prime Minister on...May 11th, 1976 issued this statement in the House of Commons:

> It is my view and the view of the Government that if the party is legal it should not be under surveillance systematically by the Royal Canadian Mounted Police or any other police. I hope that is the view of the other side of the House.

Is this the policy that you understood having been in force from 1964 on through the various governments that were in office at the time?

A. It is.

Q. Is it also an accurate statement to say that at least from 1964, as we have seen through various periods, that there was pressure or direction given to the R.C.M.P. for them to collect as much information as they could, to keep the Government informed (a) of separatists and (b) of the individuals who may want to apply for Civil Servant jobs?

A. That's correct, I think, subject to two points I would make: number one, the point you just finished making, the Parti Québecois and the other democratic parties were not subject to surveillance. So that there was always a qualification on that. The second point, I made earlier, that the R.C.M.P. were not to be limited by their own specific information, but should use all the information that was available from all sources, to try to get the maximum information possible, brought together. So that it was not just a matter for them to do alone by normal security methods. It was a bigger problem than that and there were more sources of information.

(Vol. C107, pp. 14091-3.)

92. The testimony of Mr. Robertson quoted above leads us to the following observations. First, it was not until 1976 that the instructions given the Security Service concerning the separatism movement in Quebec explicitly contained the qualification that the Parti Québecois and other democratic parties were not subject to surveillance. As we have seen, there was great confusion within the Security Service on this point for over a decade. Second, Mr. Robertson's point that the Security Service was to use other sources of information and not rely solely on "normal security methods" must be viewed in the light of other remarks he made during his testimony. For example, Mr. Robertson told us that as early as 1970, Ministers and senior officials realized that the Security Service was weak in gathering and analyzing information from open sources (Vol. C107, pp. 14093-5). Finally, we should note that Ministers and senior officials, despite their realization of the "terrible difficulty of the problem" faced by the Security Service in responding to requests for information on separatists, had effectively insulated themselves from any knowledge of how the Security Service was in fact dealing with this problem on a day-to-day basis. Consider the following excerpt from Mr. Robertson's testimony.

Q. . . . in order to bring you a policy or present to you a policy problem which could lead to a recommendation or changing of some legislation, were you not exposed to explanations as to the operations themselves, in a general way?

A. In a general way, if it would be something that would be relevant to a decision, that could be. Never about a specific case. And I think that in case the distinction seems artificial or tight, I think I should make the point that there was a very strict principle that was applied, and I hope is still applied, in security work, which was called "the need-to-know" principle; and if a person didn't need to know, he shouldn't ask and he shouldn't be told. And this was in order to maintain as tight security and information as possible. So that I was never told about a specific case and I never asked about a specific case.

(Vol. C107, p. 13854.)

93. A measure of the confusion within the ranks of the Security Service as to what the government expected with regard to its collecting information about separatism in Quebec is provided by the following extract from an R.C.M.P. audit report of the Security Screening Branch, written in 1978:

Although the most recent "H.Q." Policy statement clearly requires enquiries to be conducted to develop information reflecting on the loyalty and

reliability of an applicant or employee, "including support of the separatist cause", this policy is not being adhered to by all field commanders and investigators. Most investigators are mindful of the relevancy of separatist activity to an applicant's security status when enquiring into that individual's loyalty, but there is no concerted effort to enquire into separatist or Parti Québecois support. The expression "if it is available" was never clarified by C.C.S.I. and the resultant "H.Q." efforts to interpret it have created confusion, particularly when "H.Q." policy does not appear to coincide with the Prime Minister's public statements to the effect that the Security Service does not investigate the Parti Québecois.

This also illustrates the failure of the government's interdepartmental committee system for security and intelligence to resolve such problems.

1976-78: the search for a clearer mandate

94. Following the victory of the Parti Québecois in the Quebec provincial election on November 15, 1976, the Security Service re-evaluated its security intelligence role with respect to separatism. In December, Mr. Dare wrote to both Mr. Bourne and Mr. Robertson (the latter in his capacity of Chairman of the Interdepartmental Committee on Security and Intelligence) indicating that it was the intention of the Security Service to play the following role:

(a) adopt and maintain a low profile in discharging our mandate within Quebec;

(b) enhance our intelligence collection and monitoring capability in the province particularly with respect to [foreign interference, increasing tension among minorities, terrorist and revolutionary power bases in Quebec and penetration of the federal government by separatists who may be trying to thwart moves by the government to keep Quebec in Confederation];

(c) in accordance with our mandate continue to monitor closely the activities of subversives within legitimate political parties, groups and organizations;

(d) maintain dialogue and liaison with appropriate provincial authorities with the aim of preventing misunderstanding regarding the role of the Security Service;

(e) maintain and promote our long standing working relationship with Quebec's provincial and municipal law enforcement agencies.

With respect to foreign interference, Mr. Dare explained that the Security Service's concern was with those countries which adopt "a semi-clandestine posture in deference to federal sensitivities". He also stated that with reference to paragraph (d), he intended to meet privately and discreetly with two P.Q. Cabinet Ministers to explain the Security Service's interest in ensuring that "the democratic process is free to work, unhindered by criminal, subversive, terrorist or espionage activities".

95. Mr. Dare discussed these intentions on January 4, 1977 at a meeting chaired by Mr. Robertson and attended by Commissioner Nadon, and Messrs. Tassé, Bourne and Hall.[20] This meeting approved the security intelligence

[20] Mr. Hall was the Assistant Secretary to the Cabinet, Security, Intelligence and Emergency Planning.

programme which Mr. Dare had outlined. However, the members of the group felt that the Security Service's mandate to collect this intelligence should be clarified by a letter from the Prime Minister authorizing an interpretation of the March 27, 1975 "guidelines" broad enough "to include activities by an individual or group of a subversive as distinct from a normal political character directed toward the fragmentation of the country or designed to undermine its integrity". This group of officials thought that a new special unit being set up in the Federal-Provincial Relations Office (Mr. Tellier's group) might "ask the Security Service to obtain information". They also called for a watering-down of the commitment to close liaison with the Quebec Government and police and concluded that Mr. Dare "would reconsider" his intention to meet with Quebec Ministers.

96. Senior officers of the Security Service subsequently worked out the specific wording of "the interpretation" of the March 27, 1975 guidelines which they hoped the Prime Minister would authorize. With some alterations resulting from a meeting of Mr. Dare with Commissioner Nadon and Messrs. Bourne and Tassé, the suggested interpretation was as follows:

> 1. The Security Service will, consistent with approved Cabinet Guidelines dated 27 March 1975, subparagraphs (c) and (d), investigate:
>
> (a) individuals or groups who are suspected, on reasonable grounds, of engaging in or planning to engage in criminal, subversive, or other activities aimed at effecting the secession of any constituent of the Canadian federation;
>
> (b) accredited representatives or other agents of foreign governments, or other foreign interests, fostering by any means the secession of any constituent of the Canadian federation.
>
> 2. To accomplish the foregoing, the Security Service will be required to:
>
> (a) develop sources in the milieux relevant to 1(a) and (b);
>
> (b) direct agents in these milieux relevant to 1(a) and 1(b);
>
> (c) employ such other Security Service investigative techniques as may be necessary to obtain intelligence on persons mentioned in 1(a) and 1(b) provided that, in all of the foregoing, the Security Service will operate within the framework of the law and in accordance with government policy.

It should be noted that the words "subversive" and "other" in 1(a) have a considerable potential for expanding the March 27, 1975 guidelines.

97. The proposed interpretation of the March 27, 1975 guidelines did not receive ministerial approval. Instead, officials in the Privy Council Office drafted a letter which they proposed that Mr. Trudeau would send to Mr. Fox, the Solicitor General. Of particular relevance is the following:

> Clearly what was intended was that the Security Service should try to inform itself of activities outside the normal political process which are intended to be subversive of our system of government or of public order even if they might not have the particular characterizations referred to in [the clause in the 1975 mandate which reads "activities directed toward accomplishing governmental change within Canada or elsewhere by force or

violence or any criminal means"] and to [sic] "hostile acts against Canada" that are not necessarily motivated by a foreign power or carried through by "attack" in the usual sense of military aggression.

Mr. Fox was asked his opinion of this draft letter. He expressed a desire for much more specific authorization, but officials in his Department now raised a number of considerations about the merits of "interpreting" the mandate in the manner originally proposed by the Security Service and senior officials. They drafted a letter addressed to a Privy Council Office official for Mr. Tassé's signature raising the following questions:

> Is it in fact a proper function of one element of a national police force to collect information about a provincial government?... For how long would it be possible to keep this activity from public knowledge? In other words, is the value of the information collected going to be worth the political damage done to the Federal Government and the long-term damage which will probably be done to the R.C.M.P. by public disclosure of this activity. The R.C.M.P. cannot afford to become suspected of "political spying".

This letter went on to suggest that the R.C.M.P. Security Service should hold back on collecting intelligence with respect to Quebec separatism until Mr. Tellier's group has identified "gaps in the information which is being collected and reported about Quebec".

98. The final chapter in the search for a new mandate for the R.C.M.P. Security Service in relation to Quebec separatism was the Security Service's submission of a discussion paper entitled "National Unity Intelligence Requirements As Perceived By the R.C.M.P. Security Service". This paper was apparently requested by Mr. Gordon Robertson, who at the time was Secretary to the Cabinet for Federal-Provincial Relations. Its purpose was to advise senior government officials "on the optimum and appropriate role of the R.C.M.P. Security Service relative to the information requirements of federal policy-makers on national unity matters."

99. The discussion paper set out five options ranging from an expanded mandate to use all techniques to collect information about virtually all aspects of the Parti Québecois and the Quebec Provincial Government, to research and analysis of open information of those aspects of separatism that might fall under the existing mandate. The paper did not recommend or reject any of the options. It did point out the serious political implications of the most expansive option, and considered that:

> Enhanced collection should be supported by a public statement by the Government to the effect that all Government resources will be dedicated to the national unity question. Disclosure of enhanced R.C.M.P. Security Service activity in the national unity field without such public support could result in a harsh "backlash" against the R.C.M.P. (and the Federal) presence and activities in Quebec.

The paper also pointed out that because the analysis and research of open information would require "the acquisition of additional personnel with the necessary skills", it "could perhaps be best performed by other departments and agencies".

Conclusions

100. Throughout our analysis of Security Service policy with respect to separatism we have made a distinction between the security and the political dimensions of separatism. We have shown how neither the government nor the Security Service consistently made this distinction in the past. We realize that there are Canadians, we hope not many, who will refuse to make the distinction in the future. But we think it is a distinction which can be made and which must be made. We quote again from the Report of the Royal Commission on Security in 1969 that:

> Separatism in Quebec, if it commits no illegalities and appears to seek its ends by legal and democratic means, must be regarded as a political movement, to be dealt with in a political rather than a security context.[21]

We strongly endorse that position. Indeed we would extend it to all the parties and political groups participating in the "national unity" debate. All should be free to participate in discussions over the future of Canada and none should be the target of investigation by the security intelligence agency so long as they adhere to legal and democratic means of pursuing their aspirations.

101. The reason we take this position and endorse it strongly is the grave danger to the democratic and constitutional process of government in Canada which we believe will result from a failure or refusal to accept this position. It has been a constant theme of this Report that the heart of this nation's security is its democratic process — it is that process above all which must be secured from external attack and internal subversion. That democratic process is threatened when governments or political parties at the federal or provincial level use the methods of espionage to gain information about one another's political intentions and capabilities. Targetting a security intelligence agency against one's democratic political opponents can in itself become a threat to a most fundamental dimension of the security of Canada.

102. The principles which govern the security intelligence agency's surveillance of a separatist political party should be the same as apply to its surveillance of all other political parties. They must be the principles expressed in the Act of Parliament which establishes the agency's mandate. That Act of Parliament, as we conceive it, will establish the kinds of activity which can be the subject of surveillance by the agency. We have recommended that these activities be confined to the four categories which we described in section A of this chapter. No political party nor any group of party members should become a subject of investigation by the security intelligence agency unless there is some evidence to suggest that it or they may be participating in one or more of these four kinds of activities. Further we have recommended that the Act should prohibit the security intelligence agency from launching an investigation of any person or group of persons solely because of their involvement in lawful protest or dissent. That last principle would preclude the security intelligence agency's investigating a group or a party solely because the group or party wishes to bring about, by democratic and lawful means, changes in the

[21] *Report of the Royal Commission on Security*, 1969, para. 21.

structure of the Canadian federation, including the separation of one or more provinces.

103. The historical record provides ample evidence of the need for strict *statutory* rules with respect to the permissible limits of security intelligence surveillance. This record also shows the danger of a security intelligence agency or government officials developing their own interpretation of directives from higher authorities without confirming the validity of those interpretations. That is why our recommendations on government direction of a security intelligence agency will insist upon the accountability of the security intelligence agency to the Minister responsible for the agency and the accountability of that Minister to the Cabinet and to Parliament for the manner in which the Parliamentary standards are interpreted. We will also be recommending an independent review body to provide an additional check that surveillance by the security intelligence agency does not exceed the limits established by Parliament. In our view these controls and checks on security intelligence activities are nowhere more necessary than in relation to surveillance of members of a political party.

104. It must be emphasized that the position we have taken on this issue does *not* preclude the collection and analysis of *open* information by the security intelligence agency about democratic political parties or their members, including the Parti Québecois and its members. In this period of our history when Canadians are engaged in a passionate debate about the future of Confederation, a security intelligence agency has an important role to play in collecting and analyzing information from open sources to assess the likelihood of political violence occurring and advising both the federal and provincial governments of any threats it perceives to the use of democratic and constitutional methods of conducting and resolving this debate. The Security Service's inability to provide analysis and advice of the highest quality is one of the reasons why we will be recommending in this Report important changes in the personnel and structure of the agency responsible for security intelligence.

105. The security intelligence agency may have evidence from public sources or confidential private sources, justifying the use of more intrusive techniques for gathering information about separatists (or anti-separatists). In the following chapter we shall recommend the standards of evidence that must be met to justify the use of covert methods of information collection. At the very least, proposals to make members of a democratic political party or a provincial or municipal government the targets of covert investigative techniques must be subject to these standards and the control mechanisms for applying them. But there is a need for extra caution and consultation in using covert methods of collecting information about the members of a democratic political party or of a provincial or municipal government.

106. The question of foreign interference in the political activities associated with the constitutional debate is a particularly difficult one. In the past the R.C.M.P. Security Service has had great difficulty in distinguishing the kind of foreign intervention which constitutes a significant security threat from that which — although perhaps politically objectionable to many Canadians — is

not a security threat. In our discussion of this subject earlier in this chapter, we emphasized that it is the clandestine or deceptive nature of active measures of foreign intervention which marks them as properly subject to the surveillance of a security intelligence agency. We concede that it may often be difficult in particular circumstances to identify these measures. In doubtful cases the Director General and senior officials of the security intelligence agency should seek guidance from their Minister, the Department of External Affairs and the Interdepartmental Committee on Security and Intelligence, and ultimately from the Cabinet Committee on Security and Intelligence.

107. Finally, there is one source of confusion with respect to security intelligence activities in relation to separatism which must be removed — the conflict between the mandate to conduct surveillance and the mandate to report information for security clearance purposes. Earlier in this chapter we showed the need for consistency and coherence. The criteria which define the kinds of information the security intelligence agency must report on candidates for security clearances must be consistent with the criteria set out in the Act of Parliament which define exhaustively the activities about which the security intelligence agency may collect information.

108. In Part VII, Chapter 1 of this Report, we shall return to this question of security screening and Quebec separatism. There we take the position that, in performing its security screening responsibilities, a security intelligence agency should not collect or report information about separatists who are pursuing their cause in a legal and democratic fashion, and who, consequently, do not fall within our proposed definition of a security threat. In short, we believe that democratically committed separatists should not be regarded as a national security problem. Thus, we consider it to be outside of our terms of reference to recommend to the government whether or not such individuals should be barred from some, if not all, positions within the Federal Public Service. If the government should decide to restrict these individuals from public service employment, and further, if the government assigns an agency to collect and report information about separatists for staffing purposes, then we strongly urge that (a) this agency not be the security intelligence agency and (b) this agency not have intrusive investigatory powers. We realize that an agency without such powers will not likely identify covert separatists who seek public service employment for questionable motives. Nonetheless, the history of the last 15 years strongly suggests to us that the problems associated with covert separatists in public service jobs are insignificant when compared to those associated with active surveillance of a democratic party. Thus, the May 27, 1976 decision of the Cabinet, a decision which authorized the Security Service to report separatist information if available, for security screening purposes, should be rescinded.

(b) *Members of Parliament, election candidates, and surveillance of the Waffle*

109. As we have stated several times in this chapter, it is essential that the activities of a security intelligence agency not violate the basic principles and practices of liberal democratic government. Adherence to this principle, how-

ever, does not require exempting M.P.s or election candidates from the security intelligence process. The conviction in 1947 of a Member of Parliament, Fred Rose, for espionage demonstrated that M.P.s can perform acts damaging to national security. In so far as *investigating* M.P.s or candidates is concerned, at the very least the laws and guidelines that we shall recommend in the following chapter for the use of intrusive investigative techniques should be applied with an extra degree of caution. There is a significant difference between the investigation of 'subversives' in a private club or ethnic organization, business corporation or trade union, and the investigation of 'subversives' in political parties, especially those represented in Parliament and provincial legislatures. The competition of political parties in elections is fundamental to a democracy: for the party in power to employ a security intelligence agency to spy on its political opponents is a grave undertaking, and should be considered only where there is evidence of a serious threat to the security of Canada as defined by Parliament. In the past the Security Service and those directing it have not been sufficiently aware of the significance of such an undertaking, as testified to by some of the Security Service's activities in relation to the Parti Québecois. Nowhere is there a stronger case for control of intrusive investigative techniques, for the independent review of the use of such techniques, or for accountability to Parliament through a committee representative of all parliamentary parties, than in security intelligence activities related to M.P.s and candidates.

110. We examined many of the Security Service files on persons who were members of Parliament between 1974 and the election of May 22, 1979. This examination, together with information obtained through informal meetings with Security Service personnel, reveal that there are a number of reasons for collecting and retaining information about Members of Parliament. We think it worthwhile reviewing these reasons in order to give some indication of how the general principle we have stated above should be applied and to consider a number of policy issues that arise. In doing so we shall give some examples described in such a way as to make it most unlikely that even the M.P. concerned would be able to identify himself as the subject. The examples, of course, are based entirely upon the Security Service records. We have not necessarily included all of the information on each file. The Commission has not attempted to test the accuracy of the information. The point is not whether the information collected is true or worthwhile, but that it illustrates the various reasons put forward by the R.C.M.P. for collecting information about M.P.s. In the next chapter of our Report, we make several recommendations about the kinds of information in general that a security intelligence agency should and should not record.

111. One important reason for keeping 'security relevant information' on file on M.P.s (or candidates) is that if their party forms the government, the Prime Minister may wish to consider an M.P. for appointment to the Cabinet or as a Parliamentary Secretary. We will consider below some of the issues which arise in determining what information is 'security relevant', but there will unquestionably be cases in which the Security Service in its investigation of security threats does come upon information that is clearly security relevant.

Case 1:

— an informer reported that the M.P. was a friend of a suspected agent of a foreign country's intelligence service;

— the M.P. was visited by a diplomat who was not a suspected intelligence officer but was from another Communist country;

— The M.P.'s name and address were found among the effects of a diplomat from that country who was identified as being involved in clandestine intelligence activities.

In our view the first and third items should be kept on file about any person because it may well turn out to have operational significance in investigating the activities of a foreign intelligence agency. It should not matter that the person involved is a Member of Parliament. If the proposal which we develop later in our Report is accepted, calling for a Joint Parliamentary Committee on Security and Intelligence with access to important confidential information, the case against protecting Members of Parliament from legitimate security intelligence investigations will be even stronger. The second item should be recorded in only those cases (such as Case 1) where other information relating to a potential security threat exists. Such an item should not be recorded if it stands in isolation

112. On the other hand, if there is no security relevant information about the M.P., there is no justification for opening a file. Take for example the following case:

Case 2:

— a file was opened when an M.P. was appointed Parliamentary Secretary

— there was no other information on the file.

In this case there was clearly no justification for opening the file.

113. In a number of cases a file had been opened on a person before he became a Member of Parliament. Here again, if the file was opened because there was security relevant information on it, then it should certainly be retained after the individual is elected to Parliament. Election to Parliament should not in itself be a reason for destroying information which associates an individual with a threat to security, but if, as is true with a fair number of these files, the file was originally opened at a time when the person applied for employment with the Public Service, it is unacceptable that the file be maintained as an "M.P. file", unless there is additional security relevant information on it.

114. We turn now to the much more difficult question of what information is sufficiently relevant to security to justify its being kept on file. Our guide here must be the definition of targettable security threats which we have recommended earlier in this chapter for the statutory mandate of the security intelligence agency. Although the issues we examine here are in the context of M.P.s and candidates files, most of them apply to the retention of information about persons who are not M.P.s or candidates.

Files opened because of foreign travel and contacts with foreign diplomats

115. In many files the information recorded was about travel to Communist countries or contacts with Communist diplomats.

Case 3:

— the file was opened on the M.P. when he called on an officer of the Security Service with regard to a proposed visit to Canada of a certain group of persons from a Communist country;

— many persons who had emigrated to Canada from that country resided in the M.P.'s city;

— the M.P. and other M.P.s had visited the U.S.S.R.

Case 4:

— the file was opened on an M.P. when he declined an invitation to a Communist country's embassy reception;

— he later became a Minister and his file records contacts with Soviet bloc officials and visits to several Communist countries on official business.

Case 5:

— the file was opened on an M.P. because a woman had contacted a Communist bloc embassy on behalf of the M.P. with regard to visas for constituents;

— the M.P. had declined an invitation to a Communist country's embassy cocktail party.

Case 6:

— a file was kept active because of the M.P.'s frequent attendance at Soviet bloc embassy functions;

— the file noted that "Our sole concern in this regard is that (the M.P.) may be the target of an agent of influence campaign on the part of the Soviet bloc".

These cases raise at least two questions: first, whether the security intelligence agency should record apparently innocuous travel to Communist countries and second, whether the security intelligence agency should record apparently innocuous social or business contacts with Communist bloc embassies or officials.

116. We think that very great caution should apply to the collection and use of this foreign contact information. Our views on this point apply not only to M.P.s and candidates but to *all* persons subject to security screening. The Security Service has been known to collect systematically, information on all persons who travelled to Communist bloc countries. If information about such apparently innocuous contacts or travel is reported or is thought to be reported in the security screening process, some Canadians will be deterred from having perfectly acceptable, indeed entirely desirable, contacts with the Communist world. If it is thought that one earns a "plus mark" for declining an invitation to a reception at a Communist bloc embassy but a "minus mark" for accepting an invitation, then our politicians and other citizens, if they wish to rise to positions of responsibility in Canadian government, will be careful to avoid all contact and communication with the Communist world and its representatives.

We think this would be extremely detrimental to the opportunity of all Canadians, including their political leaders, to acquire first hand knowledge of the Communist world. No reasonable Canadian wants that result. Furthermore, we believe that it is a waste of resources for a security intelligence agency to collect and record such innocuous information, without there being additional reason for suspicion.

117. In Part VII of this Report we consider in detail the entire security screening process and make recommendations on the major policy issues. There we recommend that an independent review tribunal be established to hear appeals from those individuals whose careers have been or are suspected of having been adversely affected by federal government screening procedures. We envisage M.P.s having access to this tribunal which provides an important protection against the misuse of information in the security clearance process. The protection against the misuse of information about an M.P. who is being considered for a security sensitive position in the Cabinet or Parliament must also rest with the good judgment of his leader. The names of such M.P.s should be given to the security intelligence agency. That agency should report only information which indicates a significant association with an activity which threatens Canada's security. This information should be reported only to the Prime Minister or party leader.

118. One further point should be noted about foreign contact information. Nearly all of the information of this kind in the M.P.s' and candidates' files relates to Communist bloc countries. Many other countries, of course, have secret intelligence agencies, and none of them, so far as we can ascertain, has declared Canada off-limits. We think that the security intelligence agency should not be so preoccupied with the Communist threat as to neglect the possibility that relationships between M.P.s and non-Communist countries may also develop in a manner which threatens Canada's security. This points up the need for balance and sophistication in the direction of the security intelligence agency's targetting.

Files opened because of expression of political opinion

119. In many files on M.P.s and candidates the information included opinions expressed before or after being elected to Parliament:

Case 7:

— The file was opened on a person before he became an M.P., when he was opposed to certain policies of a foreign state;

— after he became an M.P. the file was maintained because of the possibility that certain organizations considered 'subversive' and certain foreign governments might try to influence or use him, in which case (according to the rationale expressed for maintaining the file) the Security Service should be in a position to warn him of the possibility of a compromise or of pitfalls.

Case 8:

— an M.P.'s file was opened because an article in a Communist Party newspaper reported that speeches delivered by him recognized a need for a grass-roots peace movement;

— the file contains references to views expressed by leaders of the Communist Party as to whether the Communist Party should support the M.P. or run its own candidate against him;

— the file contains the comment that "In spite of numerous references made about [the M.P.] by [the Communist Party of Canada] people, there is no firm indication of any affiliations or outward support by him for the Party". The note concluded that therefore "Little significance is. . . placed on these references";

— the reason given for maintaining the file was "to monitor any new information in the event investigation and/or interviews become necessary".

Case 9:

— a file was originally opened on a person prior to his election to Parliament when a security clearance was required. The report praised his character;

— later when he was elected to Parliament, the file was transferred to the M.P. s category of files;

— the next item on file records his public criticism of certain legislation;

— several years later the continuance of the file was justified in part by the fact that he supported "grass roots" politics.

Case 10:

— a file was opened on an M.P. because a person being interviewed by a Security Service member in a proper counterespionage operation happened to mention in a quite unrelated way that the M.P. wanted to launch a campaign to examine the activities of the R.C.M.P.

Case 11:

— a file was opened many years ago when the person was elected to a municipal body;

— when he was elected to Parliament, his election was recorded as were the results for other candidates of certain of the political parties;

— several years later, after public statements of the M.P. had been recorded on file, a review memo stated that his reputation was that he was "anti-security and anti-R.C.M.P.".

Case 12:

— a file was opened on an M.P. because, after being interviewed by a Security Service member to whom his name had been given as a reference by a person who had applied for security clearance, the R.C.M.P. officer reported that he considered the M.P. to be "somewhat officious and abrupt". The memo on file noted that the M.P.'s attitude may have been due to the fact that the House of Commons was about to meet and time was short. (The Security Service member in question advised us that he recorded his impression as it might alert someone else in a future investigation.)

120. In all of these cases (and there are others) we cannot see the security relevance of the information, whether its eventual use is for security clearance or operational purposes. Indeed the cases show that members of the Security

Service have not understood the difference between legitimate political dissent, which is essential to our democratic system, and such political advocacy or action as would constitute a threat to the security of Canada. One mistake that appears in a number of these files is the conclusion that because a person supports a policy option in Canadian politics which is also supported by the Communist Party of Canada, that person and the advocacy of the particular policy option are threats to the security of Canada. It would be just as wrong to categorize support for, say, capital punishment by a committee of Chiefs of Police as possibly subversive because it is also the position favoured by a violence-prone right-wing political group such as the Western Guard. The kind of thinking reflected in these files shows both an anti-left bias in the judgment of members of the Security Service and a tendency towards the worst kind of 'guilt by association'. Such files should be destroyed.

121. Cases 11 and 12 illustrate a particularly dangerous tendency to open files on persons who have done nothing more than take a special interest in the Security Service. Here we are reminded of the fact that one category of Security Service files is devoted to individuals who have criticized the Security Service. We think it is wrong to collect and keep information on file solely because a person has criticized or who is perceived to have criticized the security intelligence agency or has been "somewhat officious and abrupt" with one of its members. Files containing nothing more than information of this kind should be destroyed. This is not to say that the security intelligence agency should not collect information about the activities of foreign intelligence agencies or genuinely subversive groups which may be directed towards destroying the effectiveness of the security intelligence agency.

122. These files further illustrate our reasons for recommending that the security intelligence agency must be staffed and led by persons capable of better judgment than was shown in these cases. They also point to the importance of having an independent review body (a proposal we will develop in detail in Part VIII, Chapter 2) to review the agency's files periodically to make sure there is a reasonable connection between the information in its files and threats to the security of Canada as defined by Parliament.

Files opened because of associations with 'subversive' individuals or groups

123. There are numerous ways in which M.P.s and candidates may be associated with individuals or groups that are under investigation for security reasons. We believe it is impossible to formulate precisely the kind of association that may justify opening a file, but two cases may illustrate situations on either side of the line:

Case 13:

— a file was opened on an M.P. because he had a contractual arrangement with a person under investigation by the Security Service;

— a year later the M.P. was considered for appointment as a Parliamentary Secretary. It was reported that he had no adverse record;

— in 1978 the file was reviewed and destruction recommended.

Case 14:

— a file was opened on a man because it was reported that a woman suspected of being a Communist had given the man's wife's name as a reference for security screening purposes;

— when the man was elected to Parliament, the file was tranferred to the M.P. s category:

— when he was being considered for an appointment to a position where he would have access to classified information, the Security Service advised that there was "No Adverse Record" but went on to note that he had attended a Soviet reception and that some years earlier his wife had a friendship with a suspected member of the Communist Party of Canada. (This was not based on the information which had caused the file to be opened).

124. In Case 13, assuming there was reason to believe that the person was involved in an activity threatening the security of Canada, it was reasonable to keep the information about his association, since it might turn out to be important in the investigation. The information was not misused in the security clearance process and it was reasonable to recommend in 1978 that the file be destroyed. But in case 14 the association was too tenuous to justify opening a file in the first instance, and the information, which was not relevant to security, was not accurately reported when used in the security screening process.

Files opened because of personal characteristics and behaviour

125. A number of files contain information, not about political beliefs or associations, but about behaviour which, in the judgment of the Security Service, is relevant to the likelihood that an M.P. might be threatened with blackmail by a hostile foreign intelligence agency. Consider the following cases:

Case 15:

— the sole reason for opening a file on an M.P. was that his name appeared on a list, of "known or suspected homosexuals", prepared by another police force.

Case 16:

— the sole reason for a file on an M.P. was a memo recording that an informer of unknown reliability had said that a second person had told him that the M.P. was "gay";

— the security screening branch recommended that the file be retained because although the information "is inconclusive and is now of little significance. . . it could be exploited by a foreign intelligence service";

— when the M.P. was being considered for appointment to a position where he would have access to classified information, the Security Service advised, in somewhat contradictory fashion, that he had "No Adverse Record" but added "There is an unconfirmed report that he may be homosexual".

126. We believe that some of the files we have examined should not have been opened by the Security Service. We agree with Lord Denning, who, in his

Report in 1963 on the circumstances leading to the resignation of the Secretary of State for War, Mr. J.D. Profumo, made this important statement about the relationship of the behaviour of prominent public figures to security:

> All the rumours reported to me were to the effect that a Minister or person prominent in public life had been guilty of immorality or discreditable conduct of some kind or other. But it is not every piece of immorality or discreditable conduct which can be said to be a "security risk". In my opinion immorality or discreditable conduct is only a security risk if it is committed in such circumstances that it might expose the person concerned to blackmail or to undue pressures which might lead him to give away secret information.[22]

Thus, in some cases, there was no evidence recorded on the file that the behaviour of the M.P.s was in "such circumstances that it might expose the person concerned to blackmail or to undue pressures". Indeed, there was no reliable evidence on either file that the conduct was even "immoral" or "discreditable".

127. In Part VII, Chapter 1, we shall return to the question of the circumstances in which the security intelligence agency should collect and report information on the behaviour of Ministers and public servants. There we shall argue that the agency should be interested in the so-called "reliability" (as distinguished from "loyalty") dimension of security screening for the Public Service in two instances: first, when the conduct relates directly to a security threat as defined by Parliament (for example, a senior official having an affair with a suspected foreign intelligence agent); and second, when the conduct results in a significant risk of blackmail (for example, an official with access to classified information, involved with a prostitute). We think that these principles should apply to M.P.s and candidates. If they had been applied in the past, some files would not have been opened.

Briefing M.P.s on security threats

128. As we noted in a number of the cases we examined, the Security Service often collects information on an M.P.'s contacts with Soviet bloc officials so that it can warn the Member if there is reason to believe that these officials are intelligence officers using their diplomatic status as a cover for clandestine espionage or political intervention activities.

129. In principle, this type of warning or briefing is an acceptable kind of 'countering' activity. (We shall discuss the full range of countering activities in Chapter 6 of Part V.) But the security intelligence agency's briefing of M.P.s and candidates must be conducted on an open and candid basis. The M.P.s' files indicate that there has been a conscious programme on the part of the Security Service to use interviews with M.P.s arranged for one purpose (for instance, because an M.P. has been named as a reference by a person applying for a security clearance) as opportunities for conducting dialogues about the activities of Communist bloc intelligence officers. In our view, members of the security intelligence agency should approach the M.P.s with open and candid

[22] Cmnd. 2152, paragraph 294.

explanations of why they wish to speak with them. We are confident that M.P.s will understand and accept such open approaches, whereas to continue with subterfuge can only, in the long run, undermine Parliamentary confidence in the security intelligence agency.

Election candidates

130. On April 25, 1978, a newspaper report based on an anonymous letter sent to several newspapers (a copy of the letter was sent to this Commission) quoted a document purporting to be "I" Directorate (an earlier name for the Security Service) Policy Instructions dated January 1, 1971, entitled "ELECTIONS — Federal, Provincial, Municipal Subversive and Separatist Activities Within". The Security Service does not retain discarded pages from its manual. Consequently there can be no absolute confirmation that the policy as of 1971 was as indicated in the document disseminated anonymously. However, we are satisfied that it was quite probably genuine, as the content is, for all practical purposes, the same as the policy which existed throughout most of the 1970s, and which has only recently been modified.

131. The 'election policy' of January 1975 stated that field units were to report on

> All election candidates (federal, provincial and municipal) who are of significant and continuing subversive interest... regardless of their organizational affiliation, political orientation or geographic location... The term 'of subversive interest' will apply to candidates who run for office under the banner of a known subversive or separatist group or is himself a known subversive or separatist. These individuals should be the subject of a Security Service file at the Division or H.Q.'s level...
>
> Although "Election" files are of value to the security screening programme, their main purpose is to gather *statistical* information for various briefs, comparative analysis, and federal government requirements.

The information to be supplied included the percentage obtained by the candidate of the total vote cast and the identity of the official agent. In the case of a municipal election, the information was to include an assessment as to "whether or not conditions are favourable with respect to subject being able to exercise his/her political philosophy". Other information expected to be submitted as being "of intelligence value" included the identity of persons giving donations of amounts in excess of ten dollars to the candidate's campaign. A group of officers, each in charge of an operational branch of the Security Service, told us that they did not know what the words "federal government requirements" meant. We view with great alarm the Security Service having involved itself in the country's political process to this extent, even where no security problem was evident.

132. The direction given to the Security Service in May or June 1975 — that it should not investigate separatists unless their activities bring them within the six categories of activities referred to in the Cabinet Directive of March 27, 1975, — did not seem to have had any effect on the 'election policy' or the manner in which it has been carried out. In other words, until recently, reports

have been expected on any candidate who is 'known' to be a separatist in the sense that there is already a file on him.

133. The current policy as expressed in the Security Service's operational manual requires that area commanders

> Within one month following federal, provincial and municipal elections (including by-elections) submit to Headquarters a report outlining:
>
> 1. The percentage of votes obtained by each candidate on whom we have a record of activity described in [the relevant sections of the 1975 mandate which relate to "subversion".]
> 2. The impact on candidates created by groups or individuals on whom we have a record of such activity.
> 3. The impact on the results of the election created by groups or individuals on whom we have a record of [subversive] activity.

134. This policy is an improvement on the January 1975 statement cited above, provided that the 1975 mandate is not interpreted to include non-violent separatists as security threats. Our concern with the current policy, therefore, is not that it encourages improper acts so much as whether there is a genuine need for a policy on elections. If an individual identified as a security threat runs in an election, an analysis of that election should quite properly be made, evaluated and put on file. If the individual is elected, then the security intelligence agency should likely make an evaluation as to whether his new position of power implies some increased ability to endanger the security of the nation. We also believe that it is appropriate for a security intelligence agency to analyze broad political trends in the country so that it has a context in which to understand the significance of political activity which is genuinely subversive. Having said this, we see no need for a mechanical reporting process in which each field commander sends reports to Headquarters after each election. Such activity appears to us to be a poor use of security intelligence agency resources.

Surveillance of political parties: the N.D.P.'s Waffle Group

135. The Waffle came into being at the National Convention of the New Democratic Party in October 1969, when a resolution was put forward by Professor Mel Watkins and his supporters calling for an independent socialist Canada. This resolution, which became known as the Waffle Manifesto, was supported by the left wing of the Party but was defeated at the Convention. Waffle supporters continued to work as a group within the N.D.P. until the summer of 1972 when the Ontario Waffle Group was formally expelled from the provincial party. The Waffle was non-violent and did not advocate the overthrow of democratic government.

136. In November 1977, there were questions in the Ontario legislature about an alleged investigation by the R.C.M.P. of the New Democratic Party during the 1971-73 period. On December 9, 1977, the Honourable Roy McMurtry, Attorney General of Ontario, after receiving a report from the Federal Solicitor General and the R.C.M.P., told the legislature that there had not been any investigation into the activities of the New Democratic Party nor had

any entries of N.D.P. premises or offices been committed by an agent or members of the R.C.M.P. However, he was informed that the R.C.M.P. had conducted an investigation into the activities of certain members of the Waffle Group between 1970 and 1973. In his statement to the Ontario Legislature, Mr. McMurtry quoted from the R.C.M.P. report as to the reasons for the investigation:

(a) When the Waffle group came into being, it invited persons outside the N.D.P. to join its ranks. These persons included ex-members of the Communist Party of Canada and members of the Canadian Trotskyists movements. The leaders of the League for Socialist Action (Trotskyists), in fact directed their members to join the Waffle group.

(b) The R.C.M.P. investigation of certain members of the Waffle group established that subversive elements penetrated the N.D.P. through the Waffle in order to gain more respectability, credibility and influence. Although the R.C.M.P. investigation concentrated on individuals of security interest, inquiries were broadened sufficiently to put the activities of these individuals in proper perspective. The investigation was de-emphasized after the N.D.P. decided to rid itself of the Waffle. The individuals of concern to the R.C.M.P., having lost the legitimacy of membership in the N.D.P., also lost interest in the Waffle. The R.C.M.P. concern with these individuals was not reduced but any concerns that the R.C.M.P. had that these subversive elements were using the Waffle as a means of penetrating the N.D.P. and therefore as a means of acquiring credibility and influence was [sic] accordingly eliminated.

(c) During the period referred to in paragraph (b) above, the R.C.M.P. concern with individuals in the Waffle was increased when it was found that a Canadian news media person, closely associated with leading people in the Waffle, was meeting clandestinely with Konstantin Geyvandov, a Russian K.G.B. Intelligence Officer, who between August 1968 and September 1973, operated in Canada as a Pravda correspondent. The R.C.M.P. investigation confirmed that this Canadian provided reports to Geyvandov during these clandestine meetings and on at least six occasions was paid money by Geyvandov. Amongst other things, the Canadian was specifically asked by Geyvandov to provide reports to him on the N.D.P. and the Waffle.

(d) The R.C.M.P. believed that Geyvandov's purpose in seeking such reports was to assist the Russian K.G.B. Intelligence Service in deciding whether the Waffle group or any of its members were worthy of further attention by the K.G.B.

(e) Geyvandov returned to the Soviet Union in September of 1973. On January 8, 1974 the U.S.S.R. Embassy in Ottawa was advised by the Department of External Affairs that because of activities unrelated to his work as a journalist, Geyvandov would not be permitted to return to Canada.

(f) Consideration was given by the R.C.M.P. to the possibility of laying a charge against this Canadian news media person but the conclusion reached was that no charge could be laid.[23]

[23] Ontario, *Debates*, December 9, 1977.

137. Our examination of R.C.M.P. counter-subversive policies over the past decade has given us additional information on the R.C.M.P.'s interest in the Waffle Group. First of all, it is useful to place R.C.M.P. activity with regard to the Waffle in context. In the 1960s there was a shift of interest within the Counter-Subversion Branch of "I" Directorate (now the Security Service) away from the activities of Communist and front organizations to new political groups and movements which were sympathetic to the use of force or violence to achieve political purposes: student radicals of the New Left, domestic terrorists and militant members of some ethnic organizations. In addition, the Counter-Subversion Branch began to take an interest in the activities of a significant number of radicals who were non-violent in nature. The officer in charge of the Counter-Subversive Branch described some of the implications of this shift of emphasis in graphic terms in a letter to field units in September 1972. He noted that, in addition to the Communist Party and front groups, subversive activity, as defined in Canada by the Security Service, fell into two main divisions:

> ...The first division includes those individuals and organizations who constitute a violent revolutionary threat, such as Maoists, Trotskyists, violent elements of the New Left, right wing extremists, Black Power advocates, and terrorist-oriented organizations such as the F.L.Q. or urban guerrillas. Intelligence coverage and counter-measures in these cases will entail expanded human and technical source coverage, the initiation of legal action through co-operation with police agencies and government departments such as Immigration, and any such other measures deemed necessary by the Security Service to contain, defuse or neutralize the threat posed by such individuals or groups...
>
> The second primary division of interest includes essentially non-violent elements whose major strategy, whether individually or collectively, is to infiltrate or penetrate existing groups or institutions for the purpose of promoting dissident or subversive influence aimed ultimately at promoting revolutionary activity. Such elements are comprised of individuals or groups in the New Left, those in Trade Union organizations, and those in Key Sectors of society such as government, education, the mass media and political parties. It is in these areas that an increased awareness and consciousness of social change on the part of the Security Service will serve to ameliorate situations which could become polarized, extreme, and thus potential threats...

138. We find such a wide definition of subversion dangerous and unacceptable because it does not clearly distinguish radical dissent from genuine threats to Canada's security. Under our definition of security threats developed earlier in this chapter, a security intelligence agency would have no business instituting surveillance of any person or class of persons by reason only of his or their involvement in lawful protest or dissent. Indeed, we have recommended that a clause to this effect be included in the legislative mandate of the agency. Even in the case of what we have called "revolutionary subversion", meaning activities directed toward the destruction or overthrow of our liberal democratic system of government, a security intelligence agency should use only non-intrusive means to collect information on such groups or individuals unless there is some reason to suspect foreign interference, espionage, or political

violence. The other ambiguous and potentially dangerous aspect of this definition of subversion lies in the phrase "Intelligence coverage and counter-measures in these cases will entail. . . *any such other measures deemed necessary by the Security Service* to contain, defuse or neutralize the threat posed by such individuals or groups" (our emphasis). We are deeply disturbed by such an attitude, especially after hearing evidence on the Checkmate operations and other countering activities of the Security Service. We shall have more to say on countering operations in Chapter 5 of this part of our Report.

139. Given the context, then, in which the counter-subversion branch was operating, it is not surprising that the Security Service's interests in the Waffle were broader than those described in Mr. McMurtry's statement. Below is a portion of a memorandum to Divisions dated December 29, 1970 from the counter-subversion branch:

> We are obviously not interested in the normal activity of any legitimate political party as such, however, we do have a responsibility to investigate information of a potentially subversive or espionage nature within such parties. Because of its socialist nature, the NDP has always attracted subversive and radical elements in society. However, it has become increasingly apparent that these elements are now polarizing around the Waffle Group in even greater numbers, particularly in view of the willingness of the Waffle leadership to accept dissident Communists, Trotskyists and "leftists" generally in an attempt to unite the "left". Consequently, the Waffle Group is of particular interest due to the number of persons of subversive interest involved, especially on the National Leadership Committee and the National Steering Committee. As will be noted in the attachment, only ten of a total 32 individuals were elected to the Steering Committee at the Waffle National Convention. We are extremely interested in learning the identity of the remaining 22 individuals who were to be chosen as follows; two from the National Leadership Committee and 20 from the various provinces. We are also interested in the objectives of the Waffle as a group, and, together with such information as outlined in the following points, this may serve as a guideline for the submission of reports on the file "New Left Activities in Political Parties";
>
> (a) Penetration by individuals and/or groups of a subversive nature; their aims and objectives in relation to the political party. To include information on executive positions held by such persons.
>
> (b) The influence which individuals of subversive interest exert over other party members.
>
> (c) Resolutions put forward for party policy by individuals of subversive interest.
>
> (d) Recruitment activities within political parties by individuals of subversive interest.

140. In 1972, the Security Service's interest in the Waffle was premised on an additional reason — the Waffle's "extreme left posture". As well, the phrase "objectives of the Waffle as a group", quoted in the memorandum above, was more clearly defined as "National aims, strategies and planned tactics of the Waffle leadership", especially those which were not public

knowledge. Consider the following excerpt from a memorandum from the Counter-Subversion Branch, dated February 25, 1972:

> With respect to political parties, the area of primary (almost exclusive) concern at present is the N.D.P. Waffle Group. Although Security Service general interest in Waffle has been mentioned in previous correspondence to the field, we have tended to avoid delineating specific areas of interest with the result that reporting often-times deals with largely innocuous matters, much of it available through the mass media and other overt sources. It is hoped that human source coverage of Waffle will be reserved for more penetrating insight and analysis.
>
> Commencing from the premise that our interest in the movement is made obvious by the extreme left posture it has adopted, and because so many persons of interest to us have gravitated towards its ranks, it does not follow that we are interested in *all* that the Waffle Group does. That should eliminate one of the first apparent misconceptions and underline the need for greater selectivity in reporting information to H.Q.
>
> By way of broad parameters, we are interested in determining National aims, strategies and planned tactics of the Waffle leadership, especially when insights we develop go beyond their open, public announcements. That is, do they have designs which exceed their publicly declared aims and, if so, by what means (strategies) do they hope to attain them and, where possible, some estimate of their probability of success in effecting those ends would certainly place areas of concern in a more balanced perspective. Until these major, national questions are resolved, there hardly seems any point in reporting about grass roots activity, local Waffle councils, attendance at meetings, membership below executive, etc.

141. Contained in this memo is a good illustration of the Security Service's inability to distinguish radical dissent from threats to national security. A non-violent political group's "extreme left posture" should provide no rationale whatsoever for a security intelligence agency to use intrusive intelligence-gathering techniques to collect information about the group's activities and intentions. Moreover, it is even more objectionable when such a rationale is used to justify the collection of information about an element of a legitimate political party which is in opposition to the party in power.

142. A final point of interest concerning the Waffle was that the Security Service kept the Solicitor General informed of their interest in this group. A brief on the Waffle was forwarded to the Solicitor General, Mr. Goyer, and to the Privy Council Office with a letter dated March 5, 1971. The letter noted:

> Attached for your information is a secret paper prepared by the Security Service on the Waffle group of the New Democratic Party. The growing interest and participation of subversives and radical elements within this group since mid 1969, prompted the preparation of this material which has been gathered through our normal intelligence role, and not through any investigation of a particular political party.
>
> At present the Waffle is of interest from a security point of view and is rapidly becoming a faction within a political party around which radicals may polarize and subsequently be a viable political force in the N.D.P.

> The delicate position of the government in matters relating to another political party is appreciated, however, I feel you should be kept informed of these developments.

143. The brief described how the Waffle came into being, its leadership, its objectives, the support of the Waffle for the separatist movement in Quebec, and the influence of Communist and Trotskyist radicals in the group. The brief concluded:

> The prime aim of the Waffle group within the N.D.P. is the establishment of an independent socialist Canada to be achieved through the existing structure of the New Democratic Party. The Waffle Group hope to change the N.D.P. from within and radicalize the N.D.P. socialist policies.
>
> Considering the Waffle Group as a whole, it is felt that they will be a viable political force within the N.D.P. In its present relatively infant form, the Waffle Group is rapidly becoming a melting pot for radicals of all "Left" groups as well as for dissident members of the Communist Party of Canada.

Attached to the brief were notes on some individual members of the Waffle who apparently were of particular interest because they had contacts with Communist or Trotskyist front organizations. We believe that it is unnecessary and indeed undesirable to provide the Solicitor General with detailed information on individuals who are in any political party, unless of course, the information indicates that the activities of such persons are likely to threaten the security of Canada, or the investigation has reached a stage where specific action, such as a request for a warrant or the laying of a criminal charge against such individuals, is being considered. A security intelligence agency must exhibit extreme care when circulating information about individuals. In Chapter 5 of this Part, we shall be recommending the establishment of guidelines which would state explicitly the conditions under which such information should be distributed.

144. To complete our review of the surveillance of the Waffle Group by the Security Service we turn to the matter of the KGB intelligence officer mentioned by Mr. McMurtry in his earlier quoted statement to the Ontario legislature. It is both proper and necessary, in our view, for a security intelligence agency to investigate the activities of known or suspected foreign intelligence officers. Such investigations, however, should not extend to the surveillance of an entire wing of a political party where there is no evidence (as in the case of the Waffle) that it is engaged in espionage, political violence, or clandestine interference in Canadian affairs on behalf of a foreign power.

145. In conclusion, the Security Service's surveillance of the Waffle Group is an illustration of some of the major problems that have plagued Canada's security intelligence function over the past decade: the lack of vigorous review and monitoring of Security Service activities by government; the lack of a clearly defined mandate for the Security Service; and insensitivity on the part of the Security Service about what constitutes legitimate dissent in a liberal democracy and about the dangers inherent in any surveillance of a non-violent political party. All of these problems require attention if Canada is to avoid future activities akin to the Security Service's investigations of the Waffle. As we noted in our discussion earlier in this chapter on investigation of the P.Q.

and surveillance of M.P.s, a security intelligence agency must exhibit extreme caution and sensitivity in deciding to collect intelligence on those active in the political arena. In the case of the Waffle, this care and sensitivity appears to have been woefully lacking.

(c) *Colleges and universities*

146. One policy issue that *has* received a good deal of attention from Ministers and senior officials has been the conduct of security intelligence investigations in relation to the students and faculty of universities and colleges. For our purposes, the historical record here can be divided into three distinct periods:

1. 1961-1963: when the federal government established policy with regard to surveillance of universities and colleges;
2. 1964-1970: when the R.C.M.P. interpreted and applied this policy;
3. 1970-1971: when the government reviewed and refined its policy regarding surveillance of universities and colleges.

As in other sections of this chapter, our examination of this historical record is focussed on policy, not on actual operations. Two important issues stand out in this review of the past: first, the relationship of the R.C.M.P. to government in the development and implementation of security surveillance policy; and second, ministerial control of the use of informers by the Security Service.

1961-1963: the development of policy

147. During the 1950s the R.C.M.P. was preoccupied with the activities of the Communist Party and front organizations and as part of this overall programme Communist clubs and student organizations were closely monitored and a number of informants were developed. By 1960 the interest of the R.C.M.P. had broadened to include the activities of many student and faculty radicals.

148. Although student violence was not as serious a security threat in Canada as it was in Western Europe, it was watched with considerable apprehension by the R.C.M.P. security and intelligence staff. A handful of student activists were suspected to be behind the first political bombings and thefts which broke out in Montreal in 1963. A few years later there were violent confrontations in several Canadian universities. In 1968, students occupied the Administration Building at Simon Fraser University in Burnaby, B.C., and in 1969 students took over and then destroyed the computer centre at Sir George Williams University in Montreal. Many arrests were made as a result of these incidents. Also, there was evidence that violence-prone separatists in Quebec had many supporters in the universities and colleges.

149. In 1961, the Minister of Justice, the Honourable E.D. Fulton, apparently reacting to unfavourable publicity about R.C.M.P. activities on campus, gave verbal instructions to the Commissioner to suspend all investigations of subversive activities on the campuses of universities and colleges until a review of the subject could be completed. At the time, the only activities which the

R.C.M.P. deemed subversive were those of Communist organizations. Consequently, a directive issued by the R.C.M.P. on June 21, 1961, stated that all investigations connected with "Communist penetration of universities and colleges or similar institutions" were to be suspended for the time being with the exception of reports from established human sources.

150. Yet criticism of the R.C.M.P. continued. On December 14, 1962, the Honourable Donald Fleming, Minister of Justice, stated in the House that the R.C.M.P. was not developing sources on campus.[24] On January 21, 1963, the Parliamentary Secretary to the Minister of Justice stated in the House that the R.C.M.P. was not interviewing students and faculty members about the political views and activities of their colleagues.[25] In June 1963, the Council of the Canadian Association of University Teachers (C.A.U.T.) passed a resolution which criticized the R.C.M.P. and urged faculty members not to reply to questions from the R.C.M.P. as to the opinions and activities of colleagues and students.

151. On July 31, 1963, representatives from the C.A.U.T. met with Prime Minister Lester B. Pearson and the Honourable Lionel Chevrier, the Minister of Justice, to urge the new government to review the security functions of the R.C.M.P., in particular with respect to investigations carried out on university campuses. The C.A.U.T. recommended that there should be no general surveillance of the university community, that investigations should not be instituted by local officers on the basis of verbal information or press reports, that there should be no recruitment of informers in classrooms, societies or clubs, and that appropriate guidelines should be established for security clearance investigations.

152. A general review of security clearance procedures was undertaken by government at this time and on October 25, 1963, Mr. Pearson reported to the House on the policy changes that had been approved by Cabinet. (See Part VII, Chapter 1, for details of these changes).

153. On November 15, 1963, representatives of the C.A.U.T. and the National Federation of Canadian University Students met again with the Prime Minister. After this meeting a formal statement was issued on behalf of the Prime Minister, the C.A.U.T. and the President of the students' federation. It stated in part:

> There is at present no general R.C.M.P. surveillance of university campuses. The R.C.M.P. does, in the discharge of its security responsibilities, go to the universities as required for information on people seeking employment in the Public Service or where there are definite indications that individuals may be involved in espionage or subversive activities.[26]

As we shall see, this statement of policy has been reiterated by the Government of Canada on several occasions since.

---

[24] House of Commons, *Debates*, December 14, 1962, p. 2660.

[25] House of Commons, *Debates*, January 21, 1963, p. 2920.

[26] "R.C.M.P. Activities on University Campuses", *C.A.U.T. Bulletin*, Vol. 13, No. 2, October 1964.

154. At this meeting, according to Security Service files, the C.A.U.T. was advised that the Soviet Union did not hesitate to exploit university students for espionage purposes and that all known instances of this were investigated. There was also a detailed discussion on security clearance procedures since the C.A.U.T. felt that R.C.M.P. members were inept in the way they conducted investigations on campus and, in particular, that the R.C.M.P. lacked sophistication and frequently acted on the basis of rumour and unconfirmed verbal reports. Commissioner McClellan, who was also present at this meeting, was asked whether faculty and staff or students were being asked to serve as informers with respect to the opinions and activities of the members of the university community. He replied (according to the R.C.M.P. record of the meeting):

> Since 1961 the R.C.M.P. has not made this kind of inquiry on a university campus. It should be remembered that it is the information that is obtained off campus that often relates to activity on the campus.
>
> ...However, it cannot prevent university staff or even presidents of universities who are concerned with subversive activities in universities from going to the R.C.M.P. with information.

Commissioner McClellan also stated that there is "no interest in anyone's opinions or beliefs in a university except where in the field of subversion it is translated into action". The R.C.M.P. record indicates that he went on to note:

> The R.C.M.P. has operated in the field of subversion for over 40 years and are in a position to know how ideological subversion is translated into positive action. It does feel competent to differentiate between the radical and the conspirator.

155. Headquarters advised divisions, by letter dated December 24, 1963, of the meeting with the C.A.U.T. This letter did not recite Mr. Pearson's policy statement verbatim but stated that at the meeting absolute assurance had been given that there was no general security surveillance of universities or of any university organizations as such. Furthermore this letter noted the assurances given the C.A.U.T. that it was not the policy of the R.C.M.P. to ". . . permit an investigating officer to ask members of the university body, staff and/or students, to keep a general lookout for suspicious or subversive opinions or activities in university affairs". From the R.C.M.P.'s perspective Mr. Pearson's policy statement was consistent with the policy established by Mr. Fulton in 1961, a policy which virtually curtailed all R.C.M.P. investigative activity on campus with the exception of security screening inquiries.

1963-1970: interpreting and applying the policy

156. The evidence from the R.C.M.P. policy files in this period indicates that the Force believed it was unduly restricted in conducting investigations on campus, even in regard to terrorism. Thus, in Quebec, with the emergence of separatist violence, there was little effort to recruit new sources on campuses and there was no technical surveillance. In a letter dated July 8, 1968, to the Royal Commission on Security, a senior officer in the Security and Intelligence

Directorate noted that the R.C.M.P. had not been able to employ on campuses investigative procedures used prior to 1961:

> It is emphasized, however, that we continued to make use of already established sources of information, but we did not actively seek new ones. The situation remains roughly the same at present except that we are now, in fact, very cautiously endeavouring to develop a few additional sources of high reliability so that we may be in a position to continue to be informed of certain campus activities of the subversive element. However, we are not making any of these approaches on university campuses.

157. In its brief to the Royal Commission on Security in 1967, the C.A.U.T. provided confirming evidence of this cautious approach being employed by the R.C.M.P. The association observed that since 1963 no formal reports of surveillance on university campuses had reached its national office.[27] The Royal Commission on Security said in its published report that Communist subversive activity in universities and trade unions was of special significance, but did not discuss this aspect of the matter further. In the unabridged version of its Report, however, the Royal Commission noted:

> More generally, however, it is clear that as a result of government instructions originating in 1961 the security authorities do not operate as effectively in universities as they do in other areas.

158. Despite the Force's belief that the surveillance policy regarding universities was overly restrictive, we found no evidence of any serious attempt by the R.C.M.P. to have this policy reviewed by government until 1969. There is evidence, however, that the Security and Intelligence Directorate attempted to circumvent the policy. It developed a programme of accelerated 'security clearance' interviews with university faculty members with the objective of developing friendly contacts who might volunteer useful information in the future. We cannot condone the use of security clearance interviews as pretexts for developing informers even though such informers may be unpaid and may only volunteer information. If the R.C.M.P. considered that the Fulton policy (if it was ever really intended to apply for more than a year or so) was unduly restrictive, the remedy was to present the problem to government and have the policy changed. We have discussed this use of pretext interviews in more detail in Part III, Chapter 11.

1970-1971: review and refinement of government policy

159. After the October Crisis, senior officials in government were of the view that the restrictions on R.C.M.P. operations on university campuses should be relaxed. There was evidence that a significant number of terrorist sympathizers in Quebec appeared to be employed in the field of education. The question was discussed at meetings of the Law and Order Committee and the Cabinet Committee on Priorities and Planning in November 1970. In December 1970, the question was placed before Cabinet, supported by a memorandum on "Academe and Subversion" prepared by the R.C.M.P. which recommended:

> (a) that the Security Service be freed from the current restrictions governing its investigations of subversive activities at educational institutions.

[27] C.A.U.T. brief to the Royal Commission on Security, p. 28.

(b) that before such investigations are resumed, careful plans be made for making public the change in policy and the need for it; possibly to include consultations with organizations like the C.A.U.T.

Cabinet, at its meeting of December 23, 1970, agreed that the Security Service be freed from "current restrictions" provided no undertaking had been given in the past to consult with the C.A.U.T. in the event of a change in policy. The decision was not communicated to the C.A.U.T.

160. This Cabinet decision, cast as it was in general terms, seems to have been regarded by some members of the Security Service as overturning the 1963 Pearson policy. The new Solicitor General, Mr. Goyer, who was sworn in on December 20, 1970, did not view the matter in this light and as a result of his initiative the question was referred back to Cabinet, which approved the following explicit statement of policy at its meeting of September 30, 1971:

(a) that the following statement, which was agreed to by the Canadian Association of University Teachers in 1963, is confirmed as a statement of government policy regarding the activities of the R.C.M.P. on university campuses:

> "There is at present no general R.C.M.P. surveillance of university campuses. The R.C.M.P. does, in the discharge of its security responsibilities, go to the universities as required for information on people seeking employment in the public service or where there are definite indications that individuals may be involved in espionage or subversive activities."

(b) that no informers or listening devices will be used on university campuses except where the Solicitor General has cause to believe that something specific is happening beyond the general free flow of ideas on university campuses;

(c) that the current restrictions placed on the activities on university campuses of the R.C.M.P. Security Service, either written or verbal, which differ from the policy statement in (a) above be lifted forthwith;

(d) that the Solicitor General is authorized to inform the Canadian Association of University Teachers that the policy agreed to in 1963 has not been changed;

(e) that the Solicitor General make clear to representatives of the Association that while there is no policy of general surveillance on university campuses or elsewhere, the university campus would not be regarded differently from any other Canadian institutions where espionage and subversive activities were involved; and

(f) that the Cabinet decision entitled "Academe and Subversion" of December 23, 1970, be modified accordingly.

Mr. Goyer met with the C.A.U.T. on October 13, 1971 and confirmed that the 1963 policy statement was still in force. In a letter to the C.A.U.T. dated November 24, 1971, the Solicitor General added that the "university campus would not be regarded differently from any other Canadian institution when espionage and subversive activities were involved".

161. Mr. Starnes was concerned that there would be great difficulties if the Solicitor General were required to give personal approval to operations on

campus and discussed the question with Mr. Goyer and Mr. Bourne during the ensuing weeks. On December 13, 1971, the Solicitor General wrote to Commissioner Higgitt, giving his instructions as to what was required by paragraph (b) of the Cabinet decision.

> This decision means that if in the judgment of the Director General, R.C.M.P. Security Service, there is a specific requirement to use informers or listening devices as investigative aids on university campuses where there are indications that individuals may be involved in espionage or subversive activities, then the Solicitor General must agree to the requirement before the use of these investigative aids is authorized.
>
> Accordingly, I would expect to receive from the Director General R.C.M.P. Security Service a memorandum justifying the use of these investigative aids in a specific situation at a university campus on which I would note my authorization.
>
> In cases of emergency where operational necessity made it impractical or even impossible to obtain the Solicitor General's approval on time, then the Director General R.C.M.P. Security Service may authorize the use of these investigative aids and then report to me within 48 hours of the time of authorization the full circumstances of the urgent situation.
>
> I should make it clear that I do not expect this procedure to apply to those who volunteer information to the Security Service about activities on university campuses and are not paid for the information they provide. My authorization will be required, however, as stated above, for the use of paid informants as investigative aids.
>
> Since the matter of R.C.M.P. activities on university campuses has remained unsettled for a considerable length of time, I would be pleased to discuss with you your proposed instructions to the Force as soon as possible.

162. The Security Service carried out a survey to identify for approval by the Solicitor General those paid informants who were committed to inquiries on university campuses. (In 1972 there appear to have only been five such cases.) The Solicitor General was also advised that there were no listening devices of any kind deployed on university or college campuses. The Director General then informed the Minister that there were other sources who went on campus from time to time but that it was presumed they were not covered by the Cabinet Directive.

> 2. Beyond the category of those paid informants whose campus activity now requires ministerial authorization, I wish to draw to your attention those Security Service sources who, although their prime responsibilities lie elsewhere, do go onto the college and university campuses from time to time. Often, they are sent there by the organizations which they have infiltrated. An example of this type of person would be a paid agent who attends a function [of the targetted group] taking place within the university precincts and who later submits a report on the proceedings which transpired. Since the area of operations of these informants is only marginally related to campus activities in general, I have understood your correspondence and the Cabinet directive as not necessitating your prior approval for their actions. I hope you will concur that this assessment accurately reflects the full scope of the Cabinet's instructions.

We note that this seems to be a somewhat unwarranted interpretation of the Cabinet decision, even though it was accepted by the Minister. The Cabinet Directive states simply "that no informers or listening devices will be used on university campuses..." without the authorization of the Solicitor General. The same observation applies to Mr. Goyer's interpretation in his letter of December 13, 1971, referred to above, that his authorization was not necessary in the case of unpaid informers. (It is worth noting that the Senior Executive Committee of the R.C.M.P., in late 1979, decided that as a matter of policy, ministerial authorization should be sought for the use of all informers on university campuses, whether paid or not. On June 30, 1980, the Commissioner wrote to the Solicitor General informing him of this internal decision and suggesting that the matter be reviewed by Cabinet).

163. Following this exchange of correspondence between Mr. Goyer and the R.C.M.P., Mr. Starnes sent a memorandum to Divisions which interpreted the Cabinet Directive along the lines of Mr. Goyer's letter quoted above. In forwarding these instructions to the field, Mr. Starnes, stated as follows:

> The enclosed memorandum has been seen and approved by the Solicitor General.
>
> A first reading of the document may give you the impression that the effect of this new directive is to make little difference in the restrictions on Security Service investigations at universities which have existed since 1963. Though one might wish for a far freer policy in this regard, I feel that any disadvantages inherent in this policy directive are more than off-set by the fact that it is the first unequivocal statement we have had in many years covering our role in this area.
>
> Accordingly, I wish to emphasize that this directive does *not* mean that the Security Service will abandon its interest in subversive or espionage activities which occur within the confines of Canadian colleges or universities. On the contrary, now that there is a well-defined channel by which we can acquire complete authority for our presence on the campuses, I expect Division Security Service officers to intensify or maintain, as the situation warrants, our coverage of the university milieu.

164. What seems clear from our review of this period is that the R.C.M.P. felt hampered by restrictions imposed by the Minister of Justice in 1961 and by the Prime Minister in 1963, but that it chose to live with the restrictions rather than place the question before the government for clarification. Furthermore, it then circumvented what it thought to be the policy by using security screening interviews as pretexts for recruiting 'voluntary' sources on university campuses.

165. From the government's point of view, its policy on university investigations has not changed since 1963. In fact, in a letter dated January 23, 1978 to the C.A.U.T., Prime Minister Trudeau reiterated Mr. Pearson's 1963 statement and, indeed, extended it to apply not only to the R.C.M.P. but also to "all government security forces". (The C.A.U.T. had referred in earlier correspondence to an allegation that the Department of National Defence had been involved in a surveillance operation at the University of Ottawa in 1969 and 1970.) In his letter the Prime Minister added:

> I think it is important to add that, in the extremely difficult area of security operations, no person in Canada can be regarded as immune from observa-

tion or surveillance if there are reasonable grounds for believing that the person is, or has been, engaged in subversive activities. This is a point I made recently to the Leader of the Opposition in relation to a question concerning surveillance of Members of Parliament.[28]

Clearly, Mr. Trudeau's interpretation of Mr. Pearson's policy statement was not the same as that adopted by the Force throughout most of the 1960s. The R.C.M.P. believed that it was precluded from conducting virtually any investigation on campus.

166. The current policy regarding Security Service surveillance of universities and colleges appears sensible to us. The main reason for limiting the activities of the security intelligence agency on university campuses is that excessive surveillance will have a chilling effect on the freedom of discussion and debate which is an essential characteristic of the liberal university. Students and faculty must feel free to express all kinds of ideas without any fear that their views may be recorded in reports by the security intelligence agency to government. On the other hand, we agree with Prime Minister Trudeau's observation, quoted above, to the effect that no person in Canada should be regarded as immune from surveillance if there are reasonable grounds for believing that the person is participating in subversive activities, so long as "subversive activities" are defined according to the definition we have proposed in section A of this chapter. University and college campuses, as well as other valued institutions in our society, should not be treated as sanctuaries in which terrorists or secret agents of foreign powers can operate free from surveillance by the security intelligence agency. A security intelligence agency, however, should be concerned with only those acts of political violence on campuses that pose a *serious* threat to the democratic order. Most attempts by violence-prone groups to interrupt the process of rational discussion on campus appear not to fall in this category and should be handled by local police.

167. In addition to agreeing with the current policy regarding universities and colleges, we also concur with the requirement that ministerial approval should be obtained before using developed human sources (as described in the next chapter) on campuses. We say this primarily because of the dangers that an indiscriminate use of informers can pose to valued freedoms within a liberal democratic society. As one American author states:

> ... the impact of covert informant surveillance on an American citizen's sense of privacy is probably greater than the effect of an overt police contact. The fear of unknown, secret surveillance was one of the main reasons for the establishment of judicial warrant and probable cause requirements for electronic surveillance. Hence, the Church committee placed the use of informants in the category of "intrusive techniques," along with mail opening, surreptitious entries, and electronic surveillance. It found "that their very nature makes them a threat to the personal privacy and constitutionally protected activities of both the targets and of persons who communicate with or associate with the targets." One legal expert has compared "police spies" and electronic surveillance this way: "The only

[28] As cited in the C.A.U.T. brief to this Commission, Appendix 18.

> difference is that under electronic surveillance you are afraid to talk to anybody in your office or over the phone, while under a spy system you are afraid to talk to anybody at all."[29]

We shall have much more to say about the use and control of informers both in this chapter and the one which follows. In Part III, Chapter 9 we have already outlined some of the legal and policy issues relevant to this area of security intelligence and police work.

168. We wish to make one final comment about this historical review of policy with regard to universities. This episode reveals a pattern of poor communications existing between the government and the R.C.M.P. In our view, this pattern of poor communications, which we observed in the previous section on Quebec separatism and which will be evident in other sections of this chapter, is due in part to a lack of understanding, both in government and the R.C.M.P., of the proper role that Ministers and government officials should play in security intelligence. This lack of understanding in turn has led to poorly developed and under-utilized structures in government to handle security matters. We believe that when Prime Ministers, Cabinets or Ministers 'make policy' on operational matters, it is imperative that those responsible for carrying out the policy report to the responsible Minister as to how the policy is being interpreted and applied. The Minister should require the security intelligence agency to send him all interpretative bulletins and letters relating to the policy.

(d) *Labour unions*

169. It is clear that many prominent union members are convinced that the R.C.M.P. has a distorted perception of labour, that its surveillance of the labour movement has been excessive and that, at times, the R.C.M.P. has served as a tool of management. Here, for example, is an excerpt from the brief submitted to us by the Canadian Labour Congress:

> The Canadian Labour Congress has, on occasion, had reason to suspect that the R.C.M.P. attempted to infiltrate legitimate trade unions and has, at times, employed disruptive tactics in strike situations... We suggest the R.C.M.P. suffers from tunnel vision in its efforts to assess the roles of legitimate trade unions in this country. The result of this is that the force is overzealous in creating files on any union member whose activities are perceived by the R.C.M.P. as subversive. Too often, the right to dissent, when exercised, is construed as a subversive act.

The C.L.C. brief asked us to

> ... explore the degree of surveillance to which trade unions are subjected, the reasons for that surveillance and determine whether the justification for such surveillance as perceived by the military or the R.C.M.P., is real or imagined.

170. In this section, we deal with the policy of the Security Service on the scope of surveillance of labour unions. However we do not deal here with the methods which were employed nor do we deal with the activities in this area on

---

[29] John T. Elliff, *The Reform of FBI Intelligence Operations*, Princeton, N.J., Princeton University Press, 1979, p. 122.

the part of the criminal investigation side of the Force. We should add that in our third Report, we shall deal with certain specific allegations of R.C.M.P. illegalities or misconduct with regard to labour unions.

171. The interest of the Security Service in the Canadian labour movement has deep roots. Indeed, in the years immediately following World War I the major preoccupation of the intelligence side of the Force was with politically motivated violence in labour unions. In 1918 a proclamation was issued by government, under the authority of the War Measures Act, which declared illegal a number of anarchist and Communist labour organizations, such as the Industrial Workers of the World and the Workers International Industrial Union. During the inter-war years regular reports on strikes and labour violence were submitted by the field to Headquarters. Frequently, the R.C.M.P. was called in to respond to industrial unrest, most notably during the Winnipeg general strike of 1919, an event which blackened the image of the Force in the eyes of labour for years to come.

172. After World War II the policy of submitting routine reports on strikes and labour unrest was changed. Field investigators were directed to report only on those situations which indicated subversive activity or a likelihood that the R.C.M.P. would be called in to restore order. Subversive activity in the immediate post-war period was equated by the Security Service with Communist control or domination of unions or locals. In October 1960, as a result of a request for information from the Joint Intelligence Bureau (now called the Bureau of Economic Intelligence in the Department of External Affairs), Headquarters also directed divisions to report on industrial disputes in which a slow-down of production, or a strike, was likely to occur. Divisions were advised that Headquarters was "mainly concerned with Communist-inspired disputes which could have an adverse effect on the Canadian economy".

173. The policy of the Security Service with respect to labour unions has not changed significantly over the past two decades: the Security Service claims to be concerned with subversive activity within trade unions, not with the activities of unions generally. For the most part, it has equated subversion with membership in a Communist or Marxist political organization. Thus, a March 1970 policy directive stated:

> 2. Our interest in the labour field is generally confined to establishing the extent and effectiveness of subversive infiltration and domination of any labour union or organization.
>
> 3. Reports should be submitted when:
>
> (a) There is any change in the executive which would place or remove a subversive to/from a position of influence either by election or appointment.
>
> (b) There is information to indicate the union is receiving support or direction from any subversive organization.
>
> (c) Information indicates financial or moral support by a union to any subversive organization.
>
> (d) Information indicates an active subversive caucus or group exists within the union.

174. In the 1970s, the Security Service continued to investigate the penetration of the trade union movement by Communists. The Security Service also investigated the presence of criminal elements in certain unions, particularly in the construction industry in Quebec. Here is how one senior officer in the Security Service, in a letter to the division dated February 23, 1977, described the objectives of the Service in relation to labour:

> Identify and monitor the degree of penetration and/or the effectiveness of infiltration and domination of any labour organization by subversives, criminals or persons/groups intent on creating civil disorder or conducting activities aimed at disrupting or overthrowing the democratic process of Government; and, recommending preventive or remedial action.

175. Under the mandate we are proposing for the security intelligence agency, these objectives would require substantial modification. (Indeed, we believe that some of these objectives lie outside of the Security Service's current mandate.) Thus, under our proposals, it would not be enough to justify the use of intrusive investigative techniques against a member of a labour union solely on the grounds that he is a Communist or a Marxist. Rather, the agency would require some indication of activities related to espionage, sabotage, foreign interference, or serious political violence before it could use paid informers, electronic surveillance or similar intrusive means for collecting information about this person. Consequently, a Communist's becoming a member of a union executive would not be grounds for launching such an investigation. Nor would a union's receipt of financial support from a domestic Communist organization necessarily justify close attention by the security intelligence agency. In addition, "criminals or persons/groups intent on creating civil disorder" would not *per se* fall within our proposed mandate, nor would all activities "aimed at disrupting. . . the democratic process". Such a broad category might be thought to contain numerous activities — for example, a prolonged Public Service strike or a non-violent occupation of a government building — which a security intelligence agency should have no business investigating. Finally "recommending preventive or remedial action" is far too ambiguous for our liking. It might be used to justify "dirty tricks" or other questionable countering activities which we believe a security intelligence agency should not be authorized to undertake. We should add that even when there are sufficient grounds for launching an investigation of a union, the security intelligence agency must exercise caution so as to collect and report only security relevant information.

Criminal activity in labour unions

176. In the course of reporting on strikes and other labour disturbances, the Security Service often played a dual role. It covered the activities of persons considered to be subversive and it reported, usually to the C.I.B. side of the Force and sometimes to local police forces, on criminal activities that came to its attention. The reporting on crime within unions was, in a sense, a 'spin off' of regular security investigative work. The extent to which the Security Service should let itself become involved with the detection of crime and violence in unions has been debated extensively within the agency during the last few years.

177. Justification for the surveillance by the Security Service of a trade union organization in 1972 was based on the presence of serious criminal elements in construction unions. A Security Service brief prepared in 1979 described the shift in interest which had occurred within the Security Service:

> 2. Our interests in the [trade union organization] have been to determine the number and degree of influence by subversives within the organization. It was established that from 1959 to 1964 the [union] was infiltrated by subversives to a minor degree. In 1965, there were seventeen (17) subversives at the [union] convention, however, in 1968 this number was reduced to six (6) delegates.
>
> 3. During the period 1968 to 1972, the [union] was infiltrated with numerous subversives, however, their influence was of no consequence due to the fact that once their communist ideology became apparent, the general congress of the [union] took steps to have them removed from office at the next general election.
>
> 4. With the advent in 1972 of . . . , the Security Service began monitoring the union from a criminal perspective. The major threat to National Security was perceived as control by criminal elements of the . . . industry . . . The Service began collecting criminal intelligence and supplied it to the police force with local criminal jurisdiction for investigation and ultimate prosecution. As more and more criminal activity was exposed . . . [the provincial government set up a commission of inquiry]. [As a result of this commission] the key members of the . . . unions responsible for the violence on picket lines, goon squads and shylocking were publicly identified and removed from any executive position within the unions. At the same time, various unions were placed under trusteeship.

178. The mandate approved by the Cabinet in March 1975 referred to "activities directed toward accomplishing governmental change. . . by force or violence or any criminal means". As we have noted the Director General, in sending copies of the mandate to his area commanders, interpreted this broadly to mean that "the use of crime or violence to accomplish any form of change (not merely the overthrow of the federal or provincial governments as provided for in the treason provisions of the Criminal Code) will also warrant attention". And in a meeting on May 22, 1975, the Director General told his staff that the Security Service should keep abreast of activities

> which may give rise to violence and civil disorder in the labour sector be it for political/subversive reasons or be it for other reasons.

This statement left many questions unanswered and the matter was discussed again in a Security Service staff paper prepared later in the year:

> When criminal elements are able through their influence in unions to pressure governments to act in a manner favourable to them, it could be construed as falling within our mandate.
>
> If it is agreed that this is the case, how do we proceed and how far do we go? We would be clearly encroaching on or at least overlapping with our own law enforcement arm as well as those of other police forces. There is a definite possibility that if we proceed unilaterally we would risk jeopardizing operations, and cause duplication of effort, confusion and bad relations. Further, members of the Security Service by and large are not equipped

with the necessary police skills to deal with sophisticated criminals and their conspiracies.

179. In August 1979, the Labour Section of the Counter-Subversion Branch, in an extensive brief, recommended that criminal activities in the labour movement should not be investigated unless there were reasonable and probable grounds to believe that such activities could escalate to civil disorder. Local law enforcement officers, however, should be informed of these criminal activities, according to the brief. It would appear that the debate on this question within the Security Service has not been satisfactorily resolved. The brief to which we referred earlier, noted:

> The criminal activity has abated somewhat, however, a review of our source files reveals that the greatest bulk of them are still aimed at criminal intelligence and have never been re-aligned to meet the security needs of our Intelligence Requirements.

180. The failure to resolve this question within the Security Service is puzzling. We cannot see any justification for allocating resources of a security intelligence agency to the investigation of criminal activity, whether in unions or in other sectors of the community, which is not related to threats to national security. Such an allocation of resources is both inefficient and inappropriate. In the context of relations between labour and the police it is one further area of possible friction which should be avoided. Finally, we do not think the Director General's broad interpretation of the mandate in this case can be supported; whatever was meant by "governmental change" it surely does not extend to the coverage of criminal activity which occurs in labour unions and which is unrelated to security.

Labour disturbances of a national character

181. Another question as to the mandate in relation to labour is the extent to which the Security Service should report on labour disturbances of a national character which, while they may not be criminally inspired, nevertheless have the potential for the interruption of essential services and civil disorder. Examples of such situations are the formation of a "common front", as happened in Quebec in 1972, or a country-wide work stoppage in essential services such as the air line pilots and traffic controllers strike.

182. The policy on such national labour disturbances is not clear. From time to time reports have been sent to government on what were perceived as potentially explosive situations. Briefs have also been prepared on "subversive influences" within certain unions.

183. Under the mandate we have recommended for the security intelligence agency, surveillance of labour unions would not be justified solely on the grounds that a union's activity might lead to a major strike or even an industrial strike involving civil disorder. The agency should keep itself well informed through *public* sources about labour relations and union activities, just as it should be well-informed about other institutions which may play an important political role in Canada's economic life. But, under the policies we have recommended, to justify *investigative* activity there would have to be

some indication that members of a union are using union activity as a means of destroying the democratic system in Canada or clandestinely promoting the interests of a foreign power or preparing or supporting espionage, sabotage, terrorism or serious political violence. The vague references to 'subversives' within unions and "potentially explosive situations" are indicative of superficial analysis which can lead to excessive surveillance of labour union activity, and have led to it in the past.

184. The security intelligence agency should take particular care in deciding to investigate and report on activities relevant to its mandate within Public Service unions. A zealous agency runs the risk of harming the collective bargaining process between the government and Public Service unions. There does not appear to be a clear written policy on the reporting of security intelligence information regarding Public Service unions, and the arrangements between the Security Service and the Department of Labour seems to have evolved on a case by case basis. Recently, at the request of the Department of Labour, circulation of such information outside the Security Service has been terminated entirely. While we appreciate the caution being exercised here, we believe that the security intelligence agency should continue to report information, albeit with great care, about security threats within Public Service unions. No institution in this country should be regarded as a safe haven for those involved in espionage, sabotage, foreign interference or serious political violence.

Liaison programmes with labour

185. A comparatively recent development in the labour field was the implementation of an active public relations programme to improve the R.C.M.P.'s relationship with labour. On the security side of the Force there has been a willingness to attempt dialogue in appropriate situations in order to reduce confrontation. Thus, in a letter to the field in September 1972, the officer in charge of the Counter-subversion Branch suggested this strategy in relation to non-violent dissident groups:

> Forms of constructive encounters between the Security Service and moderately dissident groups or individuals could be both socially and operationally useful in defusing possible problem areas. Through a programme of increased dialogue and contact with such persons, channels of communication could be established, resulting in several and various advantages and opportunities. Through the judicious exploitation of such channels and contacts, the Security Service might act as an intermediary between dissidents and political and legal institutions, thus lessening the possibilities of alienation and confrontation; it would provide for better access to our organization and increase our operational scope and credibility with these elements; and it would render such channels available for the employment of counter-influence. Common interests on the part of dissidents might also be exploited by the Security Service acting in concert with government departments involved in youth and employment programmes and monetary grants. Those individuals and groups who could not be approached in this manner would continue to be monitored and dealt with as circumstances warrant. Similar procedures will also be employed in circumstances and

areas such as those dealing with native Indian groups as they fit mainly into the non-violent category, although in a different manner.

186. In 1974, as the result of a general study involving all elements of the R.C.M.P., it was decided to launch a systematic programme to improve the relationship between labour and the police. The objective of the Labour/Police Liaison Programme was stated in the 1977 Security Service policy instruction on labour in this way:

> Participate with the enforcement personnel in establishing and maintaining a labour-police liaison programme under the police-community relations concept; and through attendance at labour conferences and conventions and by dialogue with labour leaders, enhance our knowledge about the labour movement as an interest area to be able to provide informed analysis relative to the above stated objectives.

187. Members of the Security Service attended labour conventions and seminars, and briefings were arranged for labour leaders in collaboration with the C.I.B. side of the Force. The provision of information to labour leaders on the work of the Security Service and the C.I.B. was intended to reduce the risk of confrontation and improve contacts. The Security Service usually took the lead in arranging conferences and seminars because they were considered to have better contacts with labour than did the C.I.B.

188. The dialogue between police and labour had its problems. In several provinces difficulties were encountered and in Quebec the programme never got off the ground. In British Columbia, however, members of the R.C.M.P. met with local labour councils throughout the province and the Security Service felt that there was an interest among many labour leaders in expanding the programme. However, in March 1979 a series of articles in a Vancouver newspaper charged that the Security Service was involved in the labour liaison programme. One article alleged that the Solicitor General, in response to a reporter's inquiry, had stated that the only reason for the presence of the Security Service would be to monitor subversive activities in unions. Although the involvement of Security Service personnel in the programme was never hidden, the publicity provoked union leaders in British Columbia to comment that they would have nothing more to do with a programme in which the Security Service was involved. In April 1979 the Security Service decided to withdraw from the liaison programme entirely. Henceforth the programme would be conducted by C.I.B. personnel.

189. We do not think "constructive encounters" or "defusing programmes" are an appropriate kind of activity for a security intelligence agency. In Chapter 6 of this Part we advance our reasons for recommending that in the future the security intelligence agency not be permitted to take part in countering activities of this kind. Such liaison activities in the labour field are very apt to be misused as occasions for trading information with private employers about the alleged political proclivities of their employees. They may also damage the security agency by exposing its members to undesirable publicity.

190. To conclude, the activities of the Security Service in the labour field have followed a pattern similar to that which we have observed in other

sections of this chapter. There has been far too little government direction and review of the Security Service policies with regard to unions. Consequently, the Security Service has had to define for itself the security threats facing Canada. Using as a standard the mandate we are proposing in this chapter, we conclude that the Security Service has been overzealous in investigating 'subversive elements' in the labour field. In part, this zealotry is a result of faulty analytical and political judgment within the Security Service. But in the absence of a clearly defined mandate, there is a natural tendency for a security intelligence agency, no matter how good its analytical capabilities, to err on the side of excessive intelligence-gathering, lest it be faulted by government for not having intelligence when asked. Intelligence-gathering is not something that can be simply turned on and off like a tap. This is another reason for the importance of Parliament's establishing a coherent, comprehensive mandate for security intelligence activities in this country.

191. We should make one final point concerning the surveillance of labour unions. As with universities, labour unions are valuable elements of a liberal democratic society. We see no reason why the principle of requiring ministerial approval for the use of developed sources on university campuses should not be extended to labour unions and indeed to other valued institutions in our society. The chilling effect that the indiscriminate use of informers can have on the free flow of ideas within universities surely applies as well to other institutions, including labour unions. In the chapter which follows, we shall make several recommendations as to when a security intelligence agency should employ informers and how it should proceed in obtaining ministerial approval for their use.

(e) *Right-wing groups*

192. After World War II investigations into the whereabouts and activities of German war criminals were conducted by R.C.M.P. security units. Such persons were suspected of living under assumed identities and it was logical for the R.C.M.P. to take on the investigations. In a sense, this task was an extension of its responsibility for the internment of persons who were enemies or members of organizations declared illegal under the War Measures Act.

There has been little activity in this area during recent years. In 1977 all files on Nazi War Criminals were transferred to the Criminal Investigation Branch of the Force.

193. In the late 1960s Canada experienced the problem of political violence by anti-Communist émigré groups, usually directed against Communist bloc diplomatic missions or delegations. In February 1967, as a result of a number of bombings at Yugoslav missions in Toronto and Ottawa, the Cabinet directed that

> the R.C.M.P. be authorized, and other police forces encouraged, to intensify their surveillance over, and penetration of, right-wing extremist organizations likely to commit terrorist acts; and
>
> the federal government make known its readiness to provide, on request, guard protection to any diplomatic missions which had good reason to feel in need of it.

Following this directive, divisions were instructed to pay special attention to émigré groups that were likely to commit hostile acts against diplomatic missions or foreign visitors, especially during Expo '67. This has remained a priority of the Counter-subversion Branch which made a number of organizational changes in the early 1970s to improve its coverage of terrorist-related activities.

194. In the United States, and to a lesser extent in Canada, political groups such as the Ku Klux Klan and the American Nazi Party have been active during the past two decades. Although their efforts to achieve significant political power in Canada have so far not been successful, they have been involved in the dissemination of hate propaganda, vandalism and violent confrontations. Violent terrorist elements have emerged on the fringes of such groups.

195. A number of home-grown right-wing groups with a potential for violence have been investigated by the Security Service. One such group was the Western Guard Party which was active in Toronto in recent years. The Western Guard Party, originally called the Edmund Burke Society, was founded in Toronto in 1967. Its members were anti-Communist and many also had an anti-semitic and anti-black orientation. One of its members, Geza Matrai, came to national attention when he attacked Premier Kosygin during the latter's visit to Ottawa in October 1971. There was evidence that the Western Guard had established contacts with similar organizations in the United States and was attempting to infiltrate the Ontario Social Credit Party. Although the group never achieved any national following, the Security Service believed that it was capable of political violence. In a brief prepared in 1973 the Security Service noted:

> The Western Guard does not pose a threat to national security or to the Government; however, its propensity for aggravating potentially violent situations could create problems in the area of law and order or, as evidenced in the attack on Premier Kosygin, create an embarrassing international incident.

196. Reporting on the Western Guard began in 1967, shortly after its formation had been announced in the Toronto press. Later, the Security Service had feared that the Party was accumulating firearms and holding shooting practices. During 1970 liaison with provincial police forces was established and from then on the Metro Toronto Police and the Ontario Provincial Police were informed of planned demonstrations and disruptive activity by the Western Guard. By 1973 a more intensive investigation was launched, and in May 1975, the Security Service was able to recruit an informer who joined the Party. During the later stages of the investigation, the Security Service, in collaboration with the Metro Toronto Police, were able to use this source to gather evidence for a criminal prosecution. Although the policy of the Security Service is not to 'surface' informers, it decided to do so in this case and the informer testified at the criminal trial. We discuss the legal and policy issues related to the handling of this informer in Part III, Chapter 9.

197. On February 1, 1978, after a three-month trial, Donald Andrews, one of the leaders of the Western Guard Party, was found guilty of having explosive

substances in his possession and of conspiracy to commit arson and public mischief. Dawyd Zarytshansky, another member of the Western Guard Party, was also found guilty of similar charges. Both were sentenced to prison. After the trial, which was given much publicity, the influence of the Western Guard Party declined.

198. Under the mandate which we have recommended, groups such as the Western Guard Party, committed to race hatred and to an authoritarian philosophy of government, would be a legitimate subject of interest for the security intelligence agency. The agency should be knowledgeable about the growth and significance of such movements in Canadian political life. However, the extent to which such a movement would become the target for investigation using intrusive undercover techniques of investigation would depend on whether there is evidence of activity in support of, or leading to, espionage, sabotage, foreign interference, serious political violence or terrorism.

199. One matter that has been brought to our attention relates to the investigation of groups alleged to be spreading defamatory statements about prominent Canadians. The Security Service has been asked, from time to time, to investigate individuals or groups responsible for spreading defamatory information about Parliamentarians and persons in the Public Service of Canada. Such statements are malicious gossip or, in extreme cases, false information of the type brought to light in the United States in the Watergate investigations. The question that arises is whether such a case properly falls within the mandate of the security intelligence agency. We believe that scandalous stories about a Cabinet Minister or a senior civil servant, even if untrue, are hardly a matter of national security. Unless there is the possibility of espionage through blackmail, we are of the view that such matters properly fall within the jurisdiction of the regular police, and the Director General should decline to be of assistance. The same might be said in the case of a request to investigate a group said to be engaged in criminal activities; if the organization does not appear to fall within the mandate of the agency, the request should be declined.

200. No doubt the Director General is in a difficult position when a senior official makes a request for information which is outside the agency's mandate to collect. In Part VI, Chapter 2, we shall discuss this problem in some detail, and shall make recommendations to make it easier for the Director General to refuse improper requests. Suffice it to say now that a request coming from a Minister or a senior government official does not bring a matter within the mandate of the agency. A security intelligence agency has a distinct role to play in relation to government. It has special powers but it must exercise them only in relation to security matters. It is important that it not permit itself, and that it not be asked, to stray into areas which are properly the province of the police or of the civil courts if defamatory statements have been made.

(f) *Surveillance of Black Power and Indian groups*

Surveillance of Black Power groups

201. In the late 1960s the Security Service began to devote attention to the possibility of political violence in black communities in Canada. For the most

part this concern was a result of the Black Power movement in the United States. As one senior officer in the Counter-subversion Branch noted in a letter to an official in the Department of Manpower and Immigration in January, 1968:

> Those who concern us most are the individuals, known as "black nationalists" who knew "Black Power" as a means of maintaining obedience to an extremist racist movement which advocates violence to enable coloured communities to secure dominant political and social status. Although numerically small, the influence of these black nationalists has been witnessed in Negro communities throughout the U.S.A. Their activities, affiliations and connections in this country cannot be overlooked. We do not look upon Black Power in any of its varied interpretations as an immediate threat to the security of Canada, nor is it likely to assume major proportions in the politics of this country in the near future. Nevertheless, we believe that should a large number of militant black nationalists gain admission to Canada, they would eventually form a definite problem.

202. The Counter-subversion Branch increased its investigations within black communities following the destruction of the computer centre at Sir George Williams University in February 1969, in which black students, most of them from the Caribbean, were involved. Shortly after this incident, Deputy Commissioner Kelly was asked about Black Power militancy when he appeared before the House of Commons Standing Committee on Justice and Legal Affairs.

> Mr. Alexander [M.P.]: Mr. Chairman, I noticed that the witness indicated that they are studying Black Power. I understand that you are not studying the culture or the economic aspects of Black Power but rather the militant side of it. In that regard I would think that you are making some study of it here in Canada.
>
> Deputy Commissioner Kelly: That is right.
>
> Mr. Alexander: To what extent have you found the existence of militant Black Power in Canada and where is it concentrating?
>
> Deputy Commissioner Kelly: We think there is a direct relationship between the Black Power movement in the United States and Canada. We think that the Black Panther movement in the United States has a direct contact with certain people in Canada. We know that the movement in the United States is endeavouring to expand its relationship outside the United States. Canada, being where it is geographically, is a natural. You may recall that at the Hemispheric Conference last fall in Montreal the Black Panther people came up and at one stage of this conference they actually took over. It was only with some difficulty that the organizers got it back on the rails. Then as a result of that these same people travelled to various points in Canada, Halifax being one, and wherever they went they either created trouble at the time or laid the basis for future trouble. We are very concerned that this is going to increase and, in my mind, there is no doubt that there will be more activity in due course.[30]

[30] House of Commons, Standing Committee on Justice and Legal Affairs, May 6, 1969, pp. 890-891.

203. On June 12, 1969, the Counter-subversion Branch at Headquarters instructed field units to review the extent of their reporting on racial intelligence. Those at Headquarters believed that certain individuals whom they considered to be 'militants' were entering Canada from the United States to create dissension among the black and and native populations and that there was a significant increase in racial tension across Canada. It was in connection with the surveillance of individuals in the black community that Mr. Warren Hart was recruited by the Security Service as an informer (Vol. 143, pp.21821-30). His testimony provides evidence that certain members of the black community were intent on achieving political goals through violent means and that, indeed, several of them committed criminal acts including the theft of firearms (Vol. 143, pp.21952-3). Despite these efforts, the threat of violence from members of black communities in Canada declined by the early 1970s.

204. We now consider how Security Service surveillance of black power groups would have been affected by the mandate we are proposing in this chapter. Under this proposed mandate, the Security Service would have been justified in launching some investigations using intrusive intelligence-gathering techniques, including the use of informers. For example, the Security Service considered that the destruction of the Sir George Williams computer centre was an act of serious political violence. Having said this, we have found some evidence of a lack of sensitivity in distinguishing between dissent on the one hand and activities aimed at violent confrontations, terrorist acts or violent revolution on the other. In one paper written by the Security Service in 1972 entitled "Black Nationalism and Black Extremism in Canada" — a paper which was widely distributed not only within the Security Service but also to other federal government departments and to some foreign agencies — we find this disturbing assessment:

> Having become more conscious of their black identity, *the danger is that Canadian blacks of nationalist persuasion will become more tuned in on themselves and become more willing to protest.* The immigrant groups, particularly, under the shock of exposure to a society where whites and white values are predominant, will probably become increasingly resistant to integration and assimilation and more likely to take offence at real or imagined discrimination. (Our emphasis.)

Furthermore in this paper and indeed in some of the letters and memos we have quoted above, we are concerned about the vague references to links between foreign "militants" and blacks living in Canada. The Security Service saw these links at times as posing a grave danger to Canada, and yet there is very little analysis of the nature of these foreign "militants" and their implications for Canada. Under the proposed mandate in this chapter, the security intelligence agency should be concerned about these links only if there is a threat of espionage, sabotage, foreign interference, terrorism or serious political violence. It is not enough to refer vaguely to foreigners and describe them in such loose language as "militants".

Surveillance of the Indian movement in Canada

205. In 1973 the Security Service became interested in the danger of political violence within the Indian community. The interest was generated in part by

the formation of the American Indian Movement (A.I.M.) in the United States. A.I.M. came to public attention particularly after the confrontation at Wounded Knee, South Dakota, in February 1973. The R.C.M.P. also believed that there were links between Black Power and native leaders both in Canada and the United States.

206. On August 30, 1973 a group of approximately 150 Indians took over the offices of the Department of Indian Affairs and Northern Development in the Centennial Tower Building in Ottawa. The building was occupied for 24 hours and then was vacated in a peaceful manner; however, a number of government documents were stolen in the course of the occupation. More incidents followed. In October 1973, there was an outbreak of violence at the Caughnawaga Reserve near Montreal. In 1974, from July 22 until September 3, Indians occupied Anicinabe Park in Kenora, Ontario. On August 11, a road block was set up for one day across a provincial highway through the Bonaparte Indian Reserve near Cache Creek, B.C. Finally, a group of native activists formed a cross-country 'caravan' to publicize their grievances. The Indian Caravan arrived in Ottawa on September 29, 1974, and occupied an abandoned building on Victoria Island, northwest of the Parliament Buildings. This occupation lasted over the winter until March 1, 1975, when the building was destroyed by fire.

207. Violence marked several of these demonstrations. When the Indian Caravan, accompanied by a number of non-Indian supporters, arrived at Parliament Hill on September 30, 1974, a major confrontation with the R.C.M.P. took place. Five demonstrators were charged and two were convicted in connection with the incident.

208. In 1975 and 1976 there were further incidents, mostly in British Columbia and Alberta, but acts designed to confront authorities were on the wane. For example, in September 1976, Indian militants occupied the offices of the Band Council on the Morley Reserve in Alberta, but the occupation was short-lived and, in the opinion of the Security Service, local native leaders appeared to be opposed to the occupation.

209. Prior to 1973, the Security Service had few points of contact with native groups. After the occupation of the Centennial Towers in Ottawa on August 30, 1973 — an event which took the R.C.M.P. by surprise — the Security Service decided to devote additional resources to an investigation of Indians advocating violence in order that government might be fully briefed and forewarned of future confrontations. At this time the Security Service had information that A.I.M. organizers were visiting reserves throughout Canada and the situation was regarded as volatile. The following is an excerpt from a letter from a senior officer in the Counter-subversion Branch to field units, written in September, 1973:

> There is no domestic situation which currently equals the Indian movement in terms of unpredictable volatility. The object of this programme is to bring that situation under security control so that, as a minimum, the element of surprise will not confront us again.

210. This initiative by the Security Service did not go unquestioned. For example, the R.C.M.P. Division in British Columbia, which had a long history of working with the native people, was concerned that much past work would be jeopardized by the Security Service recruiting informers. Work on the mandate of the Security Service resulted in renewed internal questioning about the investigation of native activities. Nevertheless, the Security Service continued its interest in the Indian Movement. By 1977, in a report which was distributed to senior officers of the Departments of Indian Affairs and Northern Development, National Defence and the Solicitor General and to the Privy Council Office on problem areas in the native community in Canada, the Security Service described its role with regard to Indians as follows:

> We interpret the role of the R.C.M.P. Security Service as one of monitoring the tone and temper of the Native population in Canada for the purpose of forewarning government and law enforcement agencies of impending disorder and conflict. Within this context, it is necessary to identify subversive elements (foreign or domestic) striving to influence or manipulate Native grievances for ulterior motives. This programme is pursued through normal investigative procedures and by establishing contacts and an ongoing dialogue with every relevant sector of the Native community. Although not considered a part of our role, but resulting from this dialogue, we have been consulted periodically by Native leaders to assist with specific issues which appeared to be heading towards confrontation. In these instances, the rapport already developed by our investigators contributed to neutralizing hostilities.

211. Under the mandate which we have proposed, the Security Service would be able to investigate persons in the Indian community whose activities were directed towards serious acts of violence to achieve a political objective. The extent of involvement by a security intelligence agency should depend on the seriousness of the problem. Violence on a reserve, even though politically motivated, cannot justify a massive involvement by the security intelligence agency any more than can violence on the picket line. Very often the local police will be better able to assess the situation than the security intelligence agency. We should also note that under our proposed mandate, the security intelligence agency would not be permitted to establish "ongoing dialogue" with groups with the aim of "defusing" situations.

212. Another example of Security Service involvement in the Indian movement was an investigation that was launched into the activities of the Indian Brotherhood of the Northwest Territories (I.B.N.W.T.). In 1975 the I.B.N.W.T. published its manifesto, the Dene Declaration, proclaiming the sovereignty of the Dene Nation over a large area of the N.W.T. The Security Service had received reports of white 'radicals' working with the Dene and there were rumours that the Dene were being trained in the use of weapons and the techniques of guerrilla warfare. After conducting an investigation the Security Service reached the conclusion that the rumours of possible violence among the Dene were largely unfounded. As noted in a letter forwarded to the Department of the Solicitor General on June 20, 1978:

> The ensuing investigation has proven our apprehensions to be largely unfounded. The I.B.N.W.T. is seeking special status for the Dene within

> confederation. The methods used in pursuit of this goal — extensive lobbying and public relations campaigns — are completely legitimate. The white advisors, although exerting considerable influence, never to our knowledge, counselled violence or subversive activity; they were, furthermore, dismissed by the I.B.N.W.T. in December 1977. And with the government's decision in favor of the Alcan route, the threat of pipeline sabotage in the N.W.T. was removed...
>
> I should point out that the Security Service now regards the Dene Nation no differently that it does other legitimate native groups. We are interested in these groups only to the extent that they are involved with persons or groups who might attempt to exploit native grievances for subversive ends.

213. We think this is a reasonable conclusion to have reached, providing that "subversive ends" are not interpreted to include land claims proposals that go beyond current government policy or call for significant constitutional changes. The fusing together of activities prejudicial to national security with activities prejudicial to "national integrity" or "national unity" would point to a failure to distinguish between those who are intent on destroying the democratic system in Canada and those who seek major constitutional change within the democratic system.

214. One incident that came to our attention adversely affected the relations between the R.C.M.P. and the Indian community. At the time of the United Nations Congress on Crime, which was held in Toronto in 1975, an unclassified working paper on terrorism, which had been prepared by the R.C.M.P. for the Canadian delegation, found its way into the press. The paper contained a few paragraphs on the Indian movement, including a sentence that characterized the "Red Power" movement in Canada as the "number one menace to national stability". This paper was not the responsibility of the Security Service nor did it have any part in its preparation.

(g) *The Extra Parliamentary Opposition*

215. In January 1977, it was reported in the news media that the Solicitor General had written in June 1971, to his Cabinet colleagues with respect to certain federal employees who were suspected of being supporters of the "Extra Parliamentary Opposition" (E.P.O.) and whose loyalty was put into question. There were questions in the House about the circulation of a "blacklist" and much public attention was given to the incident. Many of the facts, including the text of the Solicitor General's letter, are already in the public domain.

216. The phrase "Extra Parliamentary Opposition" needs explanation.[31] It was first used in the 1960s by European writers to describe how the traditional institutions of parliamentary democracy could be drastically reformed, if not destroyed, by pressure from "counter or parallel institutions" representative of "the masses" rather than the establishment. The Extra Parliamentary Opposi-

[31] A description of the philosophy of the Extra Parliamentary Opposition may be found in *The New Left in Canada*, published in 1970. See particularly the chapter by Dimitrios J. Roussopoulos "Towards a Revolutionary Youth Movement and an Extra Parliamentary Opposition in Canada".

tion, as it was called, would be brought about through the development of "counter institutions" in labour unions, community groups, schools and so forth. There never was, in Canada or elsewhere, any group or organization that styled itself as the Extra Parliamentary Opposition; the phrase was merely a catchword for a philosophy of a certain type of change.

217. The Security Service, in common with other security intelligence agencies in the West, began to study student radicals of the New Left in the mid 1960s. In Canada, after the Combined Universities Campaign for Nuclear Disarmament had run its course, New Left study groups and committees became established in many universities. In 1968 and 1969, as we have noted earlier in this chapter, several violent confrontations took place at Canadian universities and colleges. In other countries there were also violent incidents involving students who battled police in the Federal Republic of Germany, France, Mexico and elsewhere.

218. The New Left was not regarded by the Security Service as a disciplined organization but rather as an amorphous group of idealistic 'revolutionary' young people. It was feared by the Security Service that the movement would find support at the grass roots level which could lead to violence and civil disorder. From 1967 to 1973 surveillance of the New Left was an important priority of the Security Service. A New Left desk, later a section, was established in the Counter-subversion Branch to co-ordinate reporting and analysis. In a few years the movement had run its course and by 1972 the Security Service reached the conclusion that it no longer represented a threat to the security of Canada. After 1973, reporting on the New Left was abandoned.

219. As we noted earlier in this chapter, during 1969 and 1970 the possible penetration of New Left radicals into labour unions, community groups, government and other key sectors of society was a matter of great interest and concern to the Security Service. There was evidence that government grants to certain community groups were being used for political purposes. Within government itself a number of documents had been leaked to the press. The Privy Council Office had asked the Security Service to investigate all such thefts and leaks of documents and in the course of these investigations former student activists fell under suspicion. The October Crisis heightened the interest of government and the Security Service in the New Left movement. The Strategic Operations Centre in the Privy Council Office, for example, had referred to the influence of the New Left and the Extra Parliamentary Opposition in its report to government in December 1970.

220. The new Solicitor General, Mr. Goyer, was conscious of New Left sympathizers in government service and it appears that he discussed the question with the Director General of the Security Service early in 1971. Mr. Goyer in fact told us that he had asked the Security Service to prepare a report on the E.P.O. phenomenon (Vol. 158, p. 24171). At any rate, the Counter-subversion Branch decided in January 1971, to prepare a report on the New Left in government. The Security Service hoped that the report would alert government to the E.P.O. problem and to the close links between some federal

employees and certain community organizations which were controlled by New Left radicals.

221. The paper prepared by the Security Service was entitled "The Changing Nature of the Threat from The New Left — Extra Parliamentary Opposition, Penetration of Government". It was classified SECRET and CANADIAN EYES ONLY. Although it had been revised and edited it was still a lengthy document running to 32 pages. The paper described the concept of the Extra Parliamentary Opposition in the following terms:

> However in the context of the New Left, E.P.O. refers to the creation of "counter" or "parallel" institutions which are opposed to, and seek the destruction of, the existing social order. The strategy is to use these parallel organizations to organize the poor and the dispossessed, the workers, and the radical students, and to boycott the normal socio-political structure, thus challenging and eroding the political legitimacy of duly elected Government in the eyes of the "oppressed".

222. The paper pointed out that the central idea of the Extra Parliamentary Opposition — the destruction of the parliamentary system — had been taken up both by radicals who sought to bring about "creative disorder" and by those advocating only moderate forms of political action. The paper described in detail the activities of Praxis Corporation, a private research organization in Toronto, which was founded in the late 1960s to support community groups and promote a higher level of citizen participation in government. Praxis, according to the paper, had come to be dominated by New Left activists and had links with community action groups in Toronto and Montreal, with the labour movement and with government agencies. Attempts by Praxis to secure government funding had been supported by certain federal government employees who were said to be sympathetic to the philosophy of the New Left. (An allegation of a break-in at the Toronto office of Praxis will be dealt with in a later Report.)

223. The paper prepared by the Security Service on the E.P.O. concluded by describing the activities of a small group of New Left supporters who were employed in federal departments or agencies. Some of these employees had formed an organization, one of whose main objectives, according to the Security Service, was to politicize tenants action groups in Ottawa. The paper stated that members of the group were involved in passing official information to persons outside the federal government and that some had used their influence to recommend other New Left supporters for positions in government service. Other federal government employees were alleged to have links with the Praxis Corporation. Despite these allegations, the paper noted that "there is as yet no direct evidence of manipulation of policy and decision-making functions in the federal government".

224. Before proceeding with the chronology of events, we wish to make several points about this E.P.O. paper. We consider it to be an inadequate analysis, inflammatory in tone, and, at times, faulty in its logic. As with other papers we have reviewed in writing this chapter, the E.P.O. paper demonstrated an insensitivity to the difference between a threat to Canada's security on the one hand and legitimate dissent on the other. The careless use of language

to create sinister impressions was one manifestation of this insensitivity. Thus, certain individuals, when they joined or attempted to influence an organization, were said to be "penetrating" it. When left-leaning people met, the group was described as a "cell". An individual attending a conference was said to be "talent spotting" as he approached like-minded individuals. Another way in which the paper failed to distinguish dissent from threats to national security was the implicit assumption of guilt by association. The logic of the paper was built around the "radical" rhetoric of several individuals. Those with left leanings who then come into contact with these individuals were assumed to be part of a wider conspiracy to alter society radically. Related to all of these shortcomings was the paper's failure to analyze the E.P.O. rhetoric carefully. The assumption throughout the paper was that "E.P.O. equals subversive activity". The fundamental question of what types of E.P.O. activity, if any, constituted threats to security was never addressed.

225. The aspect of the E.P.O. matter which we find especially objectionable, however, was the circulation outside of the Security Service of a paper which names particular individuals and records many of their thoughts without any reference to their planning or engaging in activity relating to terrorism or serious political violence. Thus the paper was a prime example of the dangers which a security intelligence agency can pose to two cherished values of our society — the right of association and the right to privacy. In addition, by making certain allegations about federal government employees, the Security Service ran the risk of harming their careers.

226. In making these criticisms of the E.P.O. paper, we do not mean to imply that a security intelligence agency should ignore a phenomenon like the New Left or the E.P.O. Rather, we are arguing that to be both useful to government and sensitive to liberal democratic principles, the agency must have a competent analytical capacity. Moreover the agency should not be left on its own to make all-important judgments about when it is appropriate to use intrusive investigative techniques to collect information about domestic groups. We shall have more to say on both of these themes in subsequent chapters of this Report.

227. The E.P.O. paper was widely circulated within the Security Service before being sent by Assistant Commissioner L.R. Parent to the Solicitor General under cover of a three-page letter dated May 12, 1971. After describing the nature of the E.P.O. threat in general terms and the activities of the Praxis Corporation, Mr. Parent concluded as follows:

> Although the number of such contacts is relatively small, probably not in excess of twenty-five, the picture presented is worrying, suggesting as it does, a conscious, although perhaps not co-ordinated, attempt by various persons to use the knowledge and the influence gained by their employment with the federal government to further their own ends. Perhaps you will wish to forward a copy of this paper to the Secretary of State for his information and, as he sees fit, comment. Also you may consider it advisable to have the Security Panel study the paper.

228. After reviewing the E.P.O. matter with Mr. Robin Bourne, the Head of the Security Planning and Research Group in his Department, the Solicitor

General decided that letters should be sent to certain of his Cabinet colleagues who had responsibility for the departments in which the persons mentioned in the E.P.O. paper were employed. Thus a letter marked "Personal and Secret" and dated June 15, 1971 was sent to five Cabinet Ministers. Attached to each letter was a list of the names of 21 federal employees listed under seven departments. The letter referred to the R.C.M.P. paper (which was not enclosed) and used much the same language to describe the E.P.O. concept, Praxis Corporation and the existence within government of a group of "campus revolutionaries". Mr. Goyer concluded:

> Though the number [of E.P.O. supporters] within the Public Service is small, probably not in excess of twenty-five, the picture presented is worrying, suggesting as it does a conscious attempt by various persons to use the knowledge and the influence gained by their employment with the federal government to further their own ends. For this reason, I have attached a list of those we suspect of being engaged in or sympathetic to E.P.O. activity in one way or another, with the recommendation that steps be taken to ensure that these people have been fully briefed as to their responsibilities for ensuring the security of government information and that their activities be watched with more than normal care.

It is worth noting that the list of federal employees was prepared in the Solicitor General's Department by the simple process of extracting from the R.C.M.P. paper the names of all persons therein mentioned who were apparently in federal employment. There was no consultation with the Security Service with respect to the letter or the list of names (Vol. 158, pp. 24132, 24138).

229. The letter was delivered to the addressees and copies were given to the Privy Council Office and the Security Service. The letter was not sent to Deputy Ministers or departmental security officers. Mr. Goyer told us that he met the Prime Minister at the time and he had advised the Prime Minister of his decision to send the letter to certain of his colleagues (Vol. 158, p. 24152). In 1977, after a copy of the letter found its way into the press, the Privy Council Office made inquiries as to what had happened to the letters and what action had been taken. The result of these inquiries was that, with only one exception, the original letter could not be found on departmental files and there was no record of any action having been taken by Ministers. Nor was the matter followed up by Mr. Goyer in 1971. He told us that in his view further action was the responsibility of each Minister (Vol. 158, pp. 24165, 24170, 24172). The matter was never discussed in the Security Panel although this had been recommended by the Security Service.

230. After questions were raised in the House in 1977, the Security Service reviewed the status of the persons named in the attachment to Mr. Goyer's letter. None of these persons was of any operational interest to the Security Service. About half the persons in the list had received security clearances in the normal way, while the remainder had either left government service or did not require a security clearance in order to carry out their duties. A file review disclosed that there was no activity on any individual files after 1972, with the exception of correspondence relating to routine security clearance matters.

231. How would a matter similar to the E.P.O. affair have been handled by the security intelligence system we are proposing? One important lesson that we have drawn from this affair is the need for guidelines on the kinds of information that a security intelligence agency can report to government. In Chapter 5 of this Part, we shall emphasize in particular the care required by the agency in reporting information about individuals. Such individuals must fall within the statutory definition of security threats. (There was no effort made in the E.P.O. affair to assess the actual threat posed by each individual mentioned in Mr. Goyer's letter.) Further, the information must be relevant to the department receiving it. If these two principles are followed, a security intelligence agency would not likely send the same information about 21 individuals to five different departments.

232. A second point concerns the role of Ministers and their deputies in security matters related to public servants. Given that deputy ministers are responsible for departmental security, a Minister should become involved in only those matters concerning a member of his exempt staff (i.e., his personal staff who are not part of the Public Service, but rather, are appointed by Order-in-Council). As well, the Minister should be briefed on a departmental security matter if it is likely that he will be asked a question in Parliament about the matter. With these exceptions, the Director General of the security intelligence agency should communicate directly with the deputy minister on a departmental security matter. In Part VII, Chapter 1 we shall recommend procedures as to how a deputy minister should exercise his responsibilities when an employee or prospective employee is alleged to be a security threat. (In the E.P.O. affair, there appeared to be little action taken by those who received Mr. Goyer's letter.) We shall also propose an appeal mechanism for those who believe that their careers have been harmed by the government's security screening process. Such an appeal mechanism was not available to those individuals named in Mr. Goyer's letter.

233. There is a further matter: the paper, without deletion except for the removal of the classification CANADIAN EYES ONLY, was distributed by the Security Service to four foreign intelligence agencies without consulting either the Solicitor General or any of his officials (Vol. 158, pp. 24166 and 24143). While the letter forwarding the paper contained the usual caveat that the material was not to be used outside the foreign agency without permission of the Security Service, we are of the view that it should have been circulated only after the names of the Canadians who were under suspicion had been deleted. We are also concerned that the Security Service, when it provides such names, has no way of controlling the subsequent utilization of the information by the foreign country. The security intelligence agency should exercise great discretion in providing foreign agencies with the names of Canadians. Under no circumstances should it provide the names of Canadians involved only in domestic movements where there is no evidence of actual or planned political violence, terrorism, espionage or foreign interference. We shall return to this question in Chapter 7 of this Part.

CHAPTER 4

INFORMATION COLLECTION METHODS

1. Because of the secrecy maintained by those who pose the most serious threats to Canada's internal security, the security intelligence agency must be authorized to employ a variety of investigative techniques to enable it to collect information. The means available to it must range all the way from studying open sources of research material and obtaining information from citizens, police forces and government agencies (foreign and domestic) to using much more covert and intrusive methods that may involve the use of powers not available under law to the ordinary citizen. In this chapter we review this wide range of intelligence collection techniques and make recommendations as to which should be available under law to the security intelligence agency and what controls should govern their use.

A. BASIC PRINCIPLES

2. The proposals set forth in this chapter on methods of investigation and their control are based on five fundamental principles which we think it important to state at the outset. They should underlie whatever system of powers and controls may be used for intelligence-gathering in the future:

(a) The rule of law must be observed. We have insisted upon adherence to the rule of law at several points earlier in this Report and we re-emphasize it here. No technique of intelligence collection should be employed which entails the violation of criminal law, other statutory law or civil law (federal, provincial or municipal). If for national security purposes it is considered essential that the security intelligence agency use an investigative technique which involves the violation of law, then those responsible for enacting laws — federal, provincial or municipal — must be persuaded to change the law so that the use of the technique by the security intelligence agency is made lawful.

(b) The investigative means used must be proportionate to the gravity of the threat posed and the probability of its occurrence. In a liberal society, which as a matter of principle wishes to minimize the intrusion of secret state agencies into the private lives of its citizens and into the affairs of its political organizations and private institutions, techniques of investigation that penetrate areas of privacy should be used only when justified by the severity and imminence of the threat to national security. This principle is particularly important when groups may be subjected to security intelligence investigations although there is no evidence that they are about to commit, or have committed, a criminal offence.

(c) The need to use various investigative techniques must be weighed against possible damage to civil liberties or to valuable social institutions. The indiscriminate use of certain techniques of investigation by a security intelligence agency, even though lawful, may do great damage to the fabric of our liberal democracy. Spying on political organizations which are critical of the status quo can have a chilling effect on freedom of association and political dissent. Similarly, the widespread, indiscriminate use as informants, of journalists, trade unionists, and professors, can do grave damage to the effective functioning of a free press, free collective bargaining, and freedom of intellectual inquiry.

(d) The more intrusive the technique, the higher the authority that should be required to approve its use. The authorizing of security intelligence officers to use various techniques of information collection must be carefully structured. The least intrusive techniques should not require any prior approval by senior authorities, but as the investigation of a group or individual intensifies, the use of more covert and intrusive techniques should require the approval of more senior officials. At the other end of the spectrum, where the most intrusive techniques of all are involved, the approval of authorities external to the agency itself should be required. Where the agency is authorized by statute under strictly defined conditions to use extraordinary techniques of investigation which would be a criminal offence if used by an ordinary citizen, the judiciary should make the authoritative determination as to whether the statutory conditions have been met.

(e) Except in emergency circumstances, the least intrusive techniques of information collection must be used before more intrusive techniques. Situations may arise in which the only opportunity for obtaining information on a subject is through the application of one or more relatively intrusive techniques. But the normal rule should be to use the least intrusive techniques first.

B. CONTROLLING THE LEVEL OF INVESTIGATION

3. In 1977 the R.C.M.P. began to develop a new system for establishing more control at the Headquarters level over Security Service investigations. The key element in this control system was the Operational Priorities Review Committee (O.P.R.C.), a committee of senior Security Service officials, and a lawyer from the Department of Justice assigned to the R.C.M.P. The terms of reference of this Committee were finally approved by the Commissioner of the R.C.M.P. in 1979.[1] This system of controlling security intelligence investiga-

---

[1] Commissioner Simmonds referred to the role of this Committee in his statements to the House of Commons Committee on Justice and Legal Affairs at *in camera* meetings of the Committee on November 24 and November 29, 1977. The O.P.R.C.'s terms of reference are classified Secret. References to the role of the Committee can be found in volumes of the record of the Commission's public hearings, e.g. in Vols. 127, 138 and 163.

tions had much in common with a system of controlling the F.B.I.'s domestic security investigations introduced by the Attorney General of the United States, Edward Levi, in 1976.[2]

4. The F.B.I. system incorporates a four-fold classification of information collection activities. First, maximum discretion is permitted at the field or desk level in the collection of information from open sources or the receiving of reports from public authorities or private citizens. At the next level, the system permits active security investigations to be launched at the field level and carried on for a limited period of time (90 days) using relatively less intrusive techniques with no higher approval than that of the senior officer in a particular regional office. The purpose of such a 'preliminary investigation' is to see if there is sufficient evidence to justify a full-scale investigation using more intrusive techniques. The extension of the level of investigation beyond 90 days, requires Headquarters approval. At the third level are 'limited investigations' involving the use of more intrusive techniques such as full-scale physical surveillance and interviewing but not the full range of intelligence collection. Investigations at this third level require the approval by the Special Agent in Charge or F.B.I. Headquarters. Finally, the level of 'full' investigation involves the use of all legally available techniques, including undercover agents and the interception of private communications. The F.B.I. requires Headquarters approval for full investigations. In the F.B.I. system, the Attorney General or his designate must be notified when full investigations are approved, and may terminate a full investigation at any time; the extension of a full investigation beyond a year requires the written approval of the Department of Justice.

5. We think that an acceptable system for controlling information collection by a security intelligence agency should distinguish three basic levels of investigation: the first leaves discretion at the field or desk level without requiring approval by senior management at Headquarters; the second requires approval by senior management of the agency; the third requires approval by the Minister responsible for the agency. The system we propose is based on this three-level approach.

---

[2] For an account of this system see John T. Elliff, *The Reform of F.B.I. Intelligence Operations*, Princeton, N.J., Princeton University Press, 1979. The "Levi Guidelines" are printed in Appendix I of this book. It is very important to note that this system of control does *not* apply to counter-espionage or counter-intelligence operations of the F.B.I. In December 1980, Attorney General Benjamin Civiletti issued guidelines entitled "The Attorney General's Guidelines on Criminal Investigations of Individuals and Organizations". These guidelines govern three types of investigations: general crimes investigations, racketing enterprises investigations and domestic security investigations. Part III, which covers domestic security investigations, reads as follows: "The Attorney General's Guidelines on Domestic Security Investigations [the "Levy Guidelines"] promulgated in 1976, shall continue to govern such investigations".

Level One: Information collection and investigation requiring only field level approval

6. We think there must be ways in which members of the security intelligence organization can collect information without being required to meet any exacting evidentiary standard or to obtain the approval of higher authorities. It would be unreasonable to require a security intelligence agency to have "reasonable and probable grounds" before it can collect information about any subject. It must start somewhere. For this reason we think it is incorrect to apply, as the 1975 Cabinet Directive does, the same evidentiary standard ("reasonable and probable grounds to believe" that an individual or group "may be engaged in or planning to engage in" an activity threatening the security of Canada) to all means of collecting information. The security intelligence agency should be authorized to initiate the collection of information both from open sources and through less intrusive techniques on a much more speculative basis. Requiring the same evidentiary standard for all kinds of information collection means either that the test will be ignored or that the agency will be deprived of the opportunity of gathering the basic information to determine whether or not it should employ the most intrusive investigative techniques.

7. At this level two types of information collection can be distinguished: information from open sources, and information of a more confidential kind which is the beginning of an investigation. The first kind of information includes public information from the news media, written publications, and attendance at public meetings. With the exception of opening files on individuals, the security intelligence agency should be able to collect and analyze information from any of these public sources so long as it relates to the agency's basic function of providing intelligence about threats to the security of Canada. The opening of files on individuals, even if the information comes from public sources, should conform to principles or guidelines. We shall elaborate on these shortly.

8. In the past the R.C.M.P. Security Service has not developed a sufficiently strong capacity to draw upon such public sources or to integrate such information with information obtained from covert sources. We think that it is essential for an effective security intelligence agency to develop a strong research capacity closely integrated with its investigative activities. The agency's research activities should provide understanding of the social, economic and political context, national and international, within which threats to Canada's internal security arise.

9. The collection of information from open sources should be directed by a planning process which reflects the intelligence priorities of the government. In Part VIII we shall propose ways in which the Cabinet and interdepartmental committees might improve their capacity to identify the government's intelligence requirements in all areas including security intelligence. The security intelligence agency should not be simply a passive recipient of these intelligence requirements. Through its monitoring of public sources of information it should alert the government to new sources of activity possibly threatening the

security of Canada, and it should be in a stronger position to analyze the extent to which certain political movements, in some quarters alleged to be subversive, are, on the contrary, contributing to the vitality and diversity of Canadian democracy.

10. The second kind of information which the members of a security intelligence agency should be able to collect at the field level without higher approval is information which can be obtained without applying intrusive techniques of investigation. Examples of sources of such information are:

- existing security intelligence agency records;
- interviews with the subject of investigation;
- information from other Canadian government agencies or police forces, but not information given by individuals or groups to the government on a confidential basis;
- information volunteered by, but not solicited from, private individuals.

The purpose of this low level, preliminary investigation is to ascertain whether there is sufficient evidence of conduct threatening the security of Canada to justify a more active and intrusive investigation. Investigative activity confined to these sources of information does not involve making inquiries about an individual in a manner which could damage the individual's reputation or interests. The information obtained from sources in government available at this stage should not include information which citizens have given to the government under conditions of confidence. We would also limit such information to that available from Canadian authorities because we think it important that information received from foreign intelligence agencies should be assessed at the Headquarters of the security intelligence agency before it is used by the agency in any way.

11. A further source of confidential information which might be available at this level of investigation is information received 'accidentally' through intrusive techniques which have been authorized for the investigation of another subject. The F.B.I. control system permits the use of existing human sources at this stage but not existing technical sources (i.e. electronic eavesdropping). We are dealing here with one aspect of the so-called 'spin-off' or accidental by-product phenomenon which will be discussed more fully in the next chapter. It is possible, for instance, that an authorized full investigation of organization A may yield information indicating that organization B may pose a serious threat to security, but a full investigation of organization B using intrusive techniques has not been authorized. In these circumstances, the system for controlling the use of intrusive investigative techniques could in effect be by-passed through exploiting this opportunity to use the incidental by-products of these techniques. Members of the agency at the field or desk level should be able to use this information in their preliminary appraisal of organization B but the use of information obtained in this way must be recorded at Headquarters, so as to facilitate the monitoring of the activity by the agency's senior management and by the independent review body.

11A. We think the surreptious trailing of individuals by the security intelligence organization is sufficiently intrusive that even when it is done for the limited purpose of "subject identification" if should be approved at Head-

quaters by a member who is at a higher level of responsibility than the most senior member in the field who is involved in the matter.

12. The F.B.I. system, as we have noted, requires that extensions of monitoring or preliminary investigations beyond 90 days be approved at Headquarters. We think that it is a sound practice, where confidential sources are being used, to require Headquarters approval for the continuation of a preliminary investigation of an individual or group beyond a set period of time. It is important that the senior management of the security organization continuously review the results of preliminary investigations to ensure that the investigative resources of the agency are properly and usefully deployed. The investigation of individuals and groups even at this low level of investigation should not be carried on indefinitely without reviewing the rationale for such investigations.

Implications for opening and maintaining files

13. There is a very widespread fear, both in Canada and in other western democracies, of the dangers to citizens which could result from the improper use of security files. Apprehension about the technical capability of the modern state to look into every nook and cranny of its citizens' lives and to retain, for unknown purposes, mountains of information about us all is reflected in the oft-heard phrase "they must have a file on me". Security intelligence agencies contribute to this apprehension: they can, and sometimes do, collect information about a very large number of individuals. The R.C.M.P. Security Services, maintains a name index which in December 1977 had 1,300,000 entries, representing 800,000 files on individuals. Access to computer technology greatly facilitates the ease with which information and opinions recorded in these files can be retrieved and correlated. Information or opinions which at the push of a button can be displayed or recorded on a computer print-out can just as readily be misused.

14. We believe that controls are needed to prevent a security intelligence agency from maintaining files on thousands of people who are not threats or potential threats to the security of Canada. To say that the agency can collect information regarding individuals as long as this information relates to the agency's mandate is so vague and loose a rule as to justify almost any collection programme. For example, as we shall describe in the chapter dealing with security screening for the Public Service (Part VII, Chapter 1), the Security Service has a long established programme for collecting information on individuals in Canada who are homosexuals. This programme is based on the premise that *some* homosexuals may be subject to blackmail should they come to occupy positions with access to security relevant information. As a second example, the Security Service has been known to open files on all Canadians who travelled to Soviet bloc countries. This and similar programmes involved the opening of files on many thousands of individuals who were not perceived as even possible threats to Canada's security. Such information collection programmes are far too indiscriminate and should never have been established.

15. A variety of controls — some governing the opening and review of files, others having to do with the reporting of information — are necessary. To prevent the establishment of such programmes in future we consider first the

question of opening a file. We believe that the security intelligence agency should establish general principles or guidelines as to when it is proper to open and maintain a file on a person. These guidelines should obviously not apply to opening files on individuals for purely administrative reasons. Thus, there should be no constraints on keeping files on agency employees or on various businessmen, consultants, or others who might be providing some administrative service to the agency. Nor should these guidelines apply to keeping files on the agency's human sources, whether voluntary or paid. With these exceptions, the security intelligence agency should open and maintain a file on a person only if at least one of the following three conditions is met:

(a) there is reason to suspect that the person has been, is, or will be engaged in activities which Parliament has defined as threats to Canada's security;

(b) there is reason to suspect that the person who is or who soon will be in a position with access to security classified information, may become subject to blackmail or may become indiscreet or dishonest in such a way as to endanger the security of Canada;

(c) the person is the subject of an investigation by the security intelligence agency for security screening purposes. (Once the investigation has been completed, the agency should not continue to add information to these files unless the information relates to category (a) or (b) above.)

16. All of these categories deserve further elaboration. Because the first category relates directly to the mandate of the security intelligence agency, there is little doubt in our minds that the agency should be allowed to collect information on individuals suspected of having a connection with a threat to security. The difficulty with this category lies in deciding what constitutes "suspicion" of a link or potential link to a security threat. For example, we believe that the agency should not collect information on all individuals who take holidays in the Soviet Union or who subscribe to a Communist newspaper. The link between such individuals and a threat to security is far too tenuous. On the other hand, it is appropriate for the agency to collect information on any individual who meets a suspected foreign intelligence officer in what appears to be a clandestine manner. The definition of suspicion may also vary depending upon the individual's position. Thus, the security intelligence agency should not collect information about a public servant whose function does not require a security clearance and who is on friendly terms in an open manner with a Soviet bloc diplomat. But if, on the other hand, the public servant holds a position with access to security classified information, such a relationship, even on an open basis, could be of legitimate interest to the agency. While there are complexities involved in interpreting the standard of evidence to apply in this category, we should emphasize that it is a far less exacting standard than the one we shall propose shortly to justify the use of intrusive investigative techniques.

17. The second category would allow the agency to collect information on those individuals (including public servants and M.P.s) who hold or are about to hold a position with the federal government with access to security classified information and whose behaviour is such that they may become dishonest or

indiscreet or likely targets for blackmail in a manner which would endanger the security of Canada. As in the first category, there is the problem of what constitutes grounds for suspicion. Under what conditions, for example, is a person a likely target for blackmail? A second problem concerns whether or not this category is too narrow. Why should the agency not be allowed to collect information about illicit behaviour on the part of individuals who *might* in future hold a position with access to security relevant information? We acknowledge the risk in preventing the agency from collecting information on such individuals. There is little doubt that some of this information might be useful at some point in the future. But we believe that the risk of abuse in collecting information on so broad a category of people — as demonstrated by the Security Service's long standing programme of collecting information on homosexuals — is far greater. The government would have no way of properly defining what the agency should and should not collect. The result would likely be a security intelligence agency which was intruding far too much into the lives of Canadians.

18. Under the third category, the agency would be allowed to retain information relating to an investigation it has undertaken in regard to a security screening case concerning immigration, citizenship, or employment in the Public Service. In conducting such an investigation, the agency may conclude that the information about the individual is not relevant to security. (It may, for example, investigate an allegation concerning an individual which turns out to be false.) Nevertheless, the agency should be allowed to retain such information because of the possibility of the same allegation recurring many years after the original security screening investigation. The agency, once it has opened such a file should not continue to feed information into it unless the information relates to the first two categories noted above.

19. In putting forward these principles to help determine when it is proper for the security intelligence agency to open and maintain files on individuals, we emphasize that these principles should not apply to groups, organizations or movements which relate to or provide a context for the agency's mandate. Thus, those within the agency should be allowed to collect material from public sources on a wide range of topics including significant political trends or movements. Some of this material will contain names of individuals — for example, a newspaper article on the likely development of a new political party in Canada. The agency should be able to keep such information so long as the names of, and information about, individuals referred to in the material are not fed into an information retrieval system, whether computerized or manual, which is used for operational or security screening purposes. The agency will obviously want to retrieve information about individuals from its administrative and source files or research files, but the storage and retrieval system which relates to that material, should be distinct from the one used when advising government about individuals whose activities relate directly to a security threat.

20. Another protection against misuse of the information should lie in the conditions under which information can be reported to those who have the power to use it in ways which may adversely affect individuals. The most

important area of concern should be the security screening process, which may result in an individual being adversely affected by a report from the security intelligence agency. To meet concerns in this area we recommend, in Part VII of the Report, the establishment of a Security Appeals Tribunal, empowered to review the case of any individual who suspects that he has been or or may have been adversely affected by an inaccurate or unfair report. Also, later in this part of the Report we make recommendations as to the conditions under which the security intelligence agency may report information to police or government authorities in Canada or abroad and recommendations that the agency be prohibited from disseminating information about individuals to the media or any non-governmental bodies, including private employers. An important function of the independent review body which we shall propose (the Advisory Council on Security and Intelligence) would be to audit security intelligence operations to ensure compliance with these reporting rules.

21. The senior management of the security intelligence agency should maintain a sound programme of file review to extract material which in no way relates to the agency's mandate, or is no longer of use, so that it can be destroyed. The R.C.M.P. Security Service has maintained such a programme in recent years. Between January 1972 and June 1977, for instance, while 501,000 new files were opened, 332,201 were destroyed. Of course, as the destruction of the files relating to Operation Checkmate indicates there is a potential for abuse in destroying as well as in opening files. We have encountered instances in which instructions have been given to destroy files in order to obliterate any record of questionable activities. File destruction should not be carried out in an *ad hoc* manner but according to a clearly established schedule and based on criteria approved by the Minister responsible for the agency.

Level Two: Investigative activity requiring Headquarters approval but not ministerial approval

22. An intermediate level of investigation, which does not employ the full range of investigative techniques available to the security intelligence agency but would go beyond the preliminary stage, involves the following:

- obtaining information from foreign agencies;
- the use of "undeveloped casual sources"[3] and interviews with persons about the subject of investigation;
- physical surveillance;
- confidential government biographical[4] information for the limited purpose of subject identification (subject to the limitations and controls we recommend later).

[3] For an explanation of this term see Part III, Chapter 9, and paragraph 62 of this chapter.

[4] For an explanation of the distinction between 'biographical' and 'personal' information see section H of this chapter.

Decisions to apply this more active and intrusive kind of investigation to a group, or to an individual who is not connected to a group which is already the subject of an approved investigation, should be made at the Headquarters level of the security intelligence agency. By Headquarters level we mean members at Headquarters who are at a higher level of responsibility than the most senior member in the field involved in the matter. Such decisions would normally be made as the result of a preliminary (level one) investigation and would have the objective of ascertaining whether there is sufficient evidence to justify a full investigation. Headquarters approval of an intermediate investigation should be for a limited time. We suggest a maximum of six months.

23. The composition of the body which approves decisions at Headquarters at this stage should be a matter for the Director General and his senior management to determine, but presumably the heads of the main operational branches would play a central role in the approval process. Decisions at this stage can lead to one of three possible courses of action: termination of the investigation, continuation of the intermediate level of investigation for another period of time, or application for authorization of a full investigation. These are important targetting decisions and it is essential that they be made after a careful review of investigative results by those in the organization best equipped to analyze the results and best able to make responsible policy decisions.

24. We realize that there should be considerable flexibility in determining which of the less intrusive techniques of investigation require Headquarters approval and which do not. Therefore we recommend that this matter be regulated by administrative guidelines rather than by statute. These guidelines should be developed by the security intelligence agency and approved by the Solicitor General. They should provide for emergency situations so that an intelligence officer in the field can take advantage of important investigative opportunities which would be lost if Headquarters approval was required. But the guidelines should provide that, in such situations, Headquarters be notified as soon as possible and not later than 48 hours after the use of the technique.

25. While the security intelligence agency's use of the methods of collecting information available to it in level one and level two investigations would not require approval outside the agency itself, there should be an effective system of *ex post facto* review of investigative activities at these levels. This system of review should involve persons outside the agency itself and should include at least the following:

(a) regular checks and audits by the independent review body (the Advisory Council on Security and Intelligence);

(b) periodic reports about the extent and distribution of activity at these levels to the Deputy Solicitor General and Solicitor General;

(c) a report of the extent and distribution of activity at these levels, at least annually, to the Cabinet Committee on Security and Intelligence and to the Parliamentary Committee on Security and Intelligence.

Level Three: Investigative activity requiring approval by the Minister, and in some cases authorization by a judge

26. Beyond the first two levels of investigation are what might be termed full investigations. These are investigations which employ any of the following methods:

(a) undercover members, human sources (beyond "undeveloped casual sources");

(b) electronic surveillance (telecommunications intercepts, planting of hidden microphones, intrusive visual surveillance by electronic means and use of dial digit recorders);

(c) surreptitious entry to search or seize (for purposes other than electronic surveillance);

(d) mail checks (examination of mail covers and opening mail);

(e) access to confidential personal information about individuals or groups held by governments or private sources.

These techniques should be used by the security intelligence agency only to the extent authorized by law. Later in this chapter we shall recommend changes in the law to make these techniques available to the agency under proper conditions and controls.

27. We believe that decisions to subject an individual or the members of an organization to any of the techniques listed above are so important, in terms of both the effective deployment of the security agency's resources and the potential impact on civil liberties, that they should be based on evidence that meets a standard defined by statute. Except in emergency circumstances, such decisions should be approved by the Solicitor General, as the Minister responsible for the agency. We should make it clear that the decisions we refer to here are ones that determine that evidence obtained through less intrusive techniques of investigation justifies intensifying the general level of investigation to the most intrusive stage. Particular techniques of investigation may require an additional level of authorization. For instance, under our recommendation the use of electronic surveillance, surreptitious entry or a mail check, or access to certain kinds of confidential information, would require judicial authorization.

28. The procedure we envisage for initiating a full investigation of an individual or group would involve three stages:

Stage 1: Approval by a committee including senior management of the security intelligence agency, and representatives of the Department of Justice and the Minister responsible for the agency.

Stage 2: Approval by the Solicitor General.

Stage 3: If the law requires a judicial warrant for the use of a technique (e.g. electronic surveillance), authorization of the use of that technique by a judge.

29. A procedure for emergency situations should be provided for. It should be possible for the Director General (or a person authorized in writing by the

Director General to act in his place) to initiate a full investigation for 48 hours, without obtaining Stage 1 or Stage 2 approval. However, the Solicitor General's approval should have to be obtained within 48 hours. If it is not obtained, the full investigation should have to be terminated. It is understood that, if the Solicitor General is absent or otherwise incapacitated, the Acting Solicitor General would be able to act in his place. The Director General should report immediately to the Minister each emergency authorization which he grants. This emergency procedure does not remove the necessity to obtain a warrant authorizing those intrusive techniques which later in this chapter we recommend require a judge's warrant.

30. The Committee at Stage 1 should include higher echelon personnel and be broader in the interests it represents than is now the case with the Security Service's Operational Priorities Review Committee. We think the Committee should normally include the Director General of the agency. If he cannot attend, he should be informed as soon as possible if the Committee approves the initiation of a full investigation, for no such proposal should go forward for ministerial approval unless it is supported by the Director General. The senior legal adviser from the Department of Justice, whose position is fully described in Part VI of this Report, should also be a member of the Committee. His particular role should be to consider whether the proposed target of a full investigation is within the statutory mandate of the agency and whether the statutory standard for a full investigation has been met. The Committee should also include a senior official from the Department of the Solicitor General to ensure that a member of the Minister's staff who is not a member of the agency is fully apprised of the factors which entered into the decision to launch an intensive investigation. We think that the Assistant Deputy Solicitor General who heads the Police and Security Branch in the Solicitor General's Department would be the most appropriate person to perform this function. The selection of the security intelligence officers for this Committee should be left to the discretion of the Director General and his senior management team. The main considerations should be the inclusion of members with operational expertise in the area of investigation concerned and of senior officers with policy-making responsibilities.

31. The Committee which reviews proposals for the initiation of full investigations should not reach its decisions by majority vote. As we have stated above, no proposal to open a full investigation should be presented for ministerial approval without the Director General's support. Moreover, if the legal adviser believes that the subject of a proposed full investigation lies outside the statutory mandate of the security agency and he is unable to persuade the Committee of this, the question of its legality should be resolved by the Deputy Attorney General. On the other hand, if the representative of the Solicitor General's Department opposes a full investigation which the Director General and his colleagues believe should be undertaken and to which the legal adviser makes no objection, the Director General should put the proposal to the Minister. The security intelligence agency should also consult the Department of External Affairs before initiating a full investigation

involving the use in Canada of certain investigative techniques directed at a foreign government or a foreign national in Canada.

32. The ministerial approval called for in this procedure would entail a major extension of direct ministerial involvement in controlling security intelligence operations. At present under section 16 of the Official Secrets Act the use of electronic surveillance for national security purposes requires the authorization of the Solicitor General. There were some who questioned this requirement when it was introduced in 1974 on the grounds that it involved a Minister to an inappropriate degree in the day-to-day operations of the Security Service. How can we now justify expanding the scope of ministerial approval for security intelligence investigations? Our justification for doing so is based on a number of related points. We believe that in a system of responsible government, responsible Ministers should be accountable for the policies of the security intelligence agency. Further, our examination of Security Service activity has led us to the conclusion that many of the most important policy decisions relative to the work of a security intelligence agency arise in the process of assessing the degree of security threat and necessary countermeasures in individual cases. A number of investigative techniques have a great potential for invading privacy and impinging on civil liberties. In this class are the planting of state-paid undercover agents in political organizations, as well as techniques that involve the exercise of extraordinary powers denied to ordinary citizens, such as electronic surveillance, the opening of mail, surreptitious entry and access to confidential information. The decision to subject an individual or group to any or all of these techniques for national security purposes is a decision with important policy implications which in our view ought to have the approval of a responsible Minister. Indeed, it is through his participation in these decisions that the Minister responsible for a security intelligence agency is most likely to have the 'window' he needs into the agency's activities.

33. Our proposals also include a check on ministerial power by requiring judicial authorization of warrants to exercise the extraordinary powers of electronic surveillance, surreptitious entry, mail checks and access to confidential government information. This proposal, it might be argued, suggests an unacceptable extension of judicial authority into decisions which should be reserved for responsible Ministers. We do not think so. Under our proposal, the judiciary's role would be to determine whether or not a statutory standard established by Parliament as a condition for exercising certain extraordinary powers has been satisfied by the facts of a particular case. In normal situations of public law, the judiciary is involved when the exercise of a power is challenged after the fact. However, because of the secrecy inherent in the exercise of investigative powers by the security intelligence agency this practice becomes unrealistic, because the person affected does not normally learn of the use of this power and therefore cannot challenge its validity. Therefore we shall recommend that judicial approval be sought as a prior condition to the use of these powers. As we see it, the ministerial role with respect to these powers is to make policy decisions. For example, the Minister must decide whether the activities of a certain country's diplomats are sufficiently suspect and dangerous to risk the diplomatic repercussions of possible exposure of security

intelligence surveillance, or whether the activities of a violence-prone group pose a sufficient threat to the country's democratic process to warrant deploying the full investigative resources of the security intelligence agency. It is primarily questions of this kind which the Solicitor General must consider in deciding whether to approve an application for a judicial warrant. He might refuse to authorize an application even though convinced that it met the statutory standard. The Solicitor General should by no means be indifferent as to whether the legal requirements were satisfied by a proposed application: on the contrary, he should not approve the application for a judicial warrant unless satisfied that the legal requirements have been met. However, our proposals give the judiciary, not the Minister (or his legal advisers), the final decision whether the law is being properly applied. In our view this would ensure the application of the rule of law to these aspects of security intelligence operations and does not depart from the appropriate distribution of responsibilities between Ministers and judges.

34. In the system we propose, at the same time that the Minister gives his *general* approval to a proposal to initiate a full investigation he may also approve a proposal to apply for a judicial warrant to use one or more *particular* techniques. He might, however, not be asked for such approval or might withhold it until other techniques not requiring a judicial warrant have been used.

35. We recognize that without some protective mechanism there is a danger in this system of ministerial control. A Minister's denial of a request to initiate a full investigation may be based on improper considerations such as the desire to protect personal friends or partisan political supporters. Because of the danger in this and other areas, we shall recommend that the Director General must have direct access to the Prime Minister when he believes that the security intelligence agency is subject to improper ministerial direction, and, in extreme circumstances when in his view his concern is not dealt with adequately by the Prime Minister, to the independent review body.

36. The approval of a full investigation should be subject to standards set out in the statute governing the security intelligence agency. The statute should provide that a full investigation may be undertaken if:

(a) there is evidence that makes it reasonable to believe that an individual or group is participating in an activity which falls within the first three categories of activity (i.e. espionage, foreign interference and political violence) described as threats to the security of Canada in the statutory mandate of the security intelligence agency; and

(b) the activity represents a present or probable threat to the security of Canada of sufficiently serious proportions to justify encroachments on individual privacy or actions which may adversely affect the exercise of human rights and fundamental freedoms recognized and declared in Part I of the Canadian Bill of Rights; and

(c) less intrusive techniques of investigation are unlikely to succeed, or have been tried and have been found to be inadequate to produce the information needed to conclude the investigation, or the urgency of the matter makes it impractical to use other investigative techniques.

37. Full investigations should be approved for a maximum of one year at a time. The extension of a full investigation beyond its authorized duration should be subject to an approval process similar to that required for the initiation of a full investigation. Granted that security investigations must by their very nature frequently be more long-term than criminal investigations, nevertheless individuals and groups should not be subjected to indefinite investigation by the state's security agency. That is why it is important to review carefully the results of a full investigation to determine whether useful information has been obtained from the techniques employed and whether there is a basis for extending the full investigation for a further period.

38. When the new system of controls comes into force it is extremely important that it be applied as quickly as possible to all existing Security Service investigations which employ the techniques covered by a full investigation. This would involve an assessment of the current investigative activity of the Security Service in the light of new standards established by Parliament. Such a review and assessment should be a top priority of the senior management of the new security intelligence agency and of the Solicitor General.

39. Besides the system of prior approval for full investigations recommended above, there should be a system of *ex post facto* review of full investigations. This system of review should have at least the following elements:

(a) regular checks and audits by the independent review body (i.e. the Advisory Council on Security and Intelligence);

(b) a report at least annually to the Cabinet Committee on Security and Intelligence and to the Parliamentary Committee on Security and Intelligence of the range of full investigations and methods used.

WE RECOMMEND THAT a system for controlling the collection of information by the security intelligence agency be established which distinguishes three levels of investigation.

(7)

WE RECOMMEND THAT investigations at the first two levels be regulated by administrative guidelines developed by the security intelligence agency and approved by the Solicitor General.

(8)

WE RECOMMEND THAT the statute governing the security intelligence agency require ministerial approval for full investigations, indicate the techniques of collection that may be used in a full investigation and stipulate that a full investigation be undertaken only if

(a) there is evidence that makes it reasonable to believe that an individual or group is participating in an activity which falls within categories of activities (a) to (c) identified, in the statute governing the security intelligence agency, as threats to the security of Canada; and

(b) the activity represents a present or probable threat to the security of Canada of sufficiently serious proportions to justify encroachments on individual privacy or actions which may adversely affect the exercise of human rights and fundamental freedoms as recognized and declared in Part I of the Canadian Bill of Rights; and

(c) less intrusive techniques of investigation are unlikely to succeed, or have been tried and have been found to be inadequate to produce the information needed to conclude the investigation, or the urgency of the matter makes it impractical to use other investigative techniques.

(9)

WE RECOMMEND THAT the security intelligence agency and the Solicitor General should move as quickly as possible to apply this system of controls to all security intelligence investigations which are under way at the time this new system of controls is introduced.

(10)

WE RECOMMEND THAT, with the exception of administrative and source files, the security intelligence agency open and maintain a file on a person only if at least one of the following three conditions is met:

(a) there is reason to suspect that the person has been, is, or will be, engaged in activities which Parliament has defined as threats to Canada's security;

(b) there is reason to suspect that the person, who is, or who soon will be, in a position with access to security classified information, may become subject to blackmail or may become indiscreet or dishonest in such a way as to endanger the security of Canada;

(c) the person is the subject of any investigation by the security intelligence agency for security screening purposes. (Once the investigation has been completed, the agency should not continue to add information to these files unless the information relates to category (a) or (b) above.)

(11)

WE RECOMMEND THAT the security intelligence agency and the independent review body (the Advisory Council on Security and Intelligence) develop programmes for reviewing agency files on a regular basis to ensure compliance with the general principles for opening and maintaining files on individuals.

(12)

WE RECOMMEND THAT the storage and retrieval system for information on individuals whose activities are relevant to the security intelligence agency's mandate be separate from those systems pertaining to administrative, source and research files.

(13)

WE RECOMMEND THAT the security intelligence agency's files, documents, tapes and other matter be erased or destroyed only according to conditions and criteria set down in guidelines approved by the Solicitor General.

(14)

WE RECOMMEND THAT the security intelligence agency consult the Department of External Affairs before initiating a full investigation involving the use in Canada of certain investigative techniques directed at a foreign government or a foreign national in Canada.

(15)

40. The foregoing section of this chapter has dealt with the *general* system of controlling the collection of information by the security intelligence agency. It was designed to encompass the use of all techniques, without regard to their special legality. We now turn to those specific techniques which at present raise legal difficulties and which, therefore, may require changes in the law. The groundwork for this part of the chapter was laid in Part III where we analyzed the legal issues raised by the investigative methods used by the R.C.M.P. Security Service and indicated whether we thought that continued use of the method in the future was justified. In what follows we now set out the details of the legal and policy changes which we think should be made with respect to particular investigative techniques employed by a security intelligence agency.

C. PHYSICAL SURVEILLANCE

41. Physical surveillance techniques are used to collect information about the movements, habits and contacts of persons by surreptitiously following them or observing their premises. In Part III, Chapter 8 we described how this technique had been developed by the R.C.M.P. Security Service and the general importance of physical surveillance operations, carried out to a large extent in the Security Service by the highly specialized Watcher Service. There is no doubt in our minds that expert physical surveillance must continue in the future to be an investigative technique available to Canada's security intelligence agency.

42. Much physical surveillance of a person's public movements and contacts is less intrusive than intercepting private communications or planting an undercover agent within an organization and should, whenever appropriate, be used before or instead of resorting to those more intrusive techniques. Still, we regard physical surveillance, whether for the limited purpose of identification or for other investigative purposes, as sufficiently intrusive to justify requiring approval at Headquarters (level two). When publicly financed surveillance teams, fully equipped and expertly trained, are directed to follow a person surreptitiously, noting every movement and contact, there should be reasonable grounds for believing that such a person, whether a citizen, a visitor or a diplomat, poses a threat, even unwittingly, to national security.

43. We think it would be wise, whenever practicable, for the security intelligence agency to continue to use specialized teams, such as the Watcher Service, for physical surveillance operations. Not only are such teams most likely to have the skill necessary to overcome the security measures employed by 'hard' targets in the espionage and terrorist fields, but also they can be better trained to minimize the risk of traffic accidents and other hazards associated with physical surveillance work. In locations where it is not feasible to use specialized teams, individuals who might be called upon to engage in surveillance work should continue to receive the most thorough training possible.

44. But more than a high standard of training and the maintenance of specialized teams will be needed if physical surveillance is to be carried on in the future on a satisfactory basis by our security intelligence agency. As we reported in Part III, Chapter 8, physical surveillance for both security and regular police investigations is very likely to involve a number of legal violations. At the conclusion of that chapter we took the position that, even though the legal violations resulting from physical surveillance operations may often be regarded as "minor infractions" or "technical breaches" of "merely regulatory laws", the continuation of physical surveillance without any changes in the law endangers the rule of law, for it implies that our security agency or police forces may in their institutional practices pick and choose the laws which they will obey. We argued that to permit a national police force or security intelligence agency to adopt a policy which entails systematic violations of "minor" laws puts these organizations at the top of a slippery slope and therefore that changes should be made in the law so that physical surveillance may be carried on without jeopardizing the rule of law.

45. A possible alternative to legal amendments is the establishment of a policy by attorneys general of not prosecuting surveillance team members who contravene legislation in the course of their duties. We reject this alternative. Such a policy would do nothing to resolve the dilemma of a government agency maintaining a practice that systematically involves the commission of illegal acts. Furthermore, a firm policy of non-prosecution might be rejected by the courts as an improper fettering of the attorney general's prosecutorial discretion. Thus we think the only proper alternative is to make appropriate changes in the relevant laws.

46. As was explained in Part III the laws which present difficulties in physical surveillance operations fall broadly into three categories: "rules of the road", the identification of persons and property, and trespass. Many of the laws which are apt to be violated in these areas are provincial statutes or municipal by-laws. One possible approach to these legal difficulties would be the enactment of federal legislation to provide with respect to both federal and provincial laws either a defence in defined circumstances or a procedure for authorizing what otherwise would be proscribed. Such provisions could be included in the legislation establishing the security intelligence agency. This approach would have the advantage of immediately providing a uniform legislative scheme across the country. However, we have serious doubts about the constitutionality of such an approach. It is far from clear that 'national security' or 'the security of Canada' (or, for that matter, 'national policing') constitutes a distinct subject matter of legislation over which the federal parliament has an exclusive or paramount authority. Even if these legal doubts can be set aside, we question the wisdom of unilateral action at the federal level exempting a national security intelligence organization (or a national police force) from provincial legislation. We think that unilateral federal action of this kind would undermine the possibility of fostering the kind of federal-provincial co-operation which in our view is essential to an effective system of national security in the Canadian federation. Moreover, we think it likely that the legislative changes needed to reconcile physical surveillance activities with

the rule of law may be needed just as much by provincial or municipal police forces as by a national security intelligence agency. Therefore we recommend the enactment of legislation by the Parliament of Canada to deal with breaches of federal laws and that the provinces be asked to enact provincial legislation to deal with violations of provincial and municipal laws.

The specific amendments

(a) *Rules of the road*

47. In Part III, Chapter 8 we reported that no evidence was before us to suggest that Criminal Code offences relating to the operation of motor vehicles have been committed or need to be committed by those engaged in physical surveillance. Therefore our recommendations for specific legislative amendments in this area are confined to provincial driving offences and municipal by-law infractions.

48. We think that provincial driving offences are best dealt with by the enactment by provincial legislatures of a defence available to a defined class of persons. Peace officers (a term including the R.C.M.P., provincial and municipal police forces) would be within this class, as would any other person designated (according to the function he performs) by provincial attorneys general upon the advice of the federal Solicitor General. These designated persons should include members of a security intelligence agency who regularly perform surveillance functions or who may be called upon to perform such functions. This statutory defence should be available only where a breach of traffic legislation occurs in the course of the driver's otherwise lawful duties, and the driver acts reasonably in all the circumstances, with due regard for the safety of others. We believe that the inclusion of these conditions in the legislation is necessary to ensure that the defences are not too broad. Section 3(4) of the New Brunswick Police Act[5] provides the following defence:

> A member of the Royal Canadian Mounted Police or a member of a police force shall not be convicted of a violation of any Provincial Statute if it is made to appear to the judge before whom the complaint is heard that the person charged with the offence committed the offence for the purpose of obtaining evidence or in carrying out his lawful duties.

We consider that this formulation is too broad in its scope to be applied to a security intelligence agency. Moreover, it lacks any requirement of necessity or of reasonable conduct.

49. At the same time as the recommended defence is introduced, a mechanism should be put in place which will both protect the defined class of person from personal liability in the event of actionable damage to a third party and provide an aggrieved third party with a means of recovering compensation in a proper case. Such a mechanism would recognize that the object of the statutory defence is not to deny redress to an innocent individual. On the other hand, individuals carrying out surveillance responsibilities should not be personally

[5] New Brunswick Police Act, Stats. N.B. ch.P-9.2 (1977).

liable where damage ensues, caused by what would otherwise be a breach of statute, provided that they act reasonably in the discharge of their otherwise lawful duties and with due regard for the property and the safety of others. To attach personal liability to such individuals would be unfair. We therefore consider that the federal government should accept responsibility for compensation to aggrieved persons through the ordinary civil process in the courts or through an agency similar to provincial Criminal Injuries Compensation Boards. The secrecy of the surveillance operation could be maintained by the use of *in camera* hearings in either case. The quantum of damages should in any such case be determined with reference to the same principles which guide the civil courts in such matters.

50. Violations of municipal by-laws, primarily "non-moving" and pedestrian violations, should also be dealt with in the same manner as provincial driving offences by seeking provincial co-operation to amend Municipal Acts or other relevant legislation.

(b) *Laws governing the identification of persons and property*

51. Legislation in this field exists both at the federal and provincial level. Consequently, we recommend that both federal and provincial governments be involved in amending their respective enactments. We would suggest that a provision be added to relevant legislation to permit the Director General of the security intelligence agency, or a senior officer designated in writing by the Director General, to apply to the senior government official charged with the administration of an enactment (e.g. the Superintendent of Motor Vehicles in the case of highway traffic legislation) to obtain identification or registration documents that will enable a surveillance operation to remain covert. The application would be accompanied by a sworn statement that the documents are reasonably necessary for the operation. Such identification should be deemed to comply with the requirements of the statute in question. For example, a driver's licence which contains false information will nonetheless be deemed to be a valid driver's licence, if it is applied for and granted pursuant to this provision. In the provinces where they are necessary, provisions should also be enacted to ensure that it shall not be an offence for an individual in defined circumstances to hold two valid licences (e.g. one in the individual's true name, and one in an assumed name) or to sign a specially obtained licence with other than one's usual signature. A record of all applications for 'false documentation' permits should be kept for periodic examination by the Solicitor General of Canada and by the attorneys general or solicitors general of the provinces where such applications are made.

52. The requirement in some provinces that an individual register his proper name upon entering a hotel can, we think, be safely relaxed in order to permit members conducting surveillance to register under a false name in the course of an investigation. It is our understanding that these registration laws were originally intended to allow the police to keep track of transients and to ensure that guests would not defraud hotel owners. Neither of these objects is affected by permitting members conducting surveillance to register under false names. We feel that there is no need for prior authorization in this situation; a

statutory defence enacted at the provincial level is the appropriate mechanism. The defence should be available to peace officers and other persons designated by provincial attorneys general on the advice of the federal Solicitor General who register in a hotel using a false name and address if they do so in good faith and if the use of a false identity is necessary for the performance of their lawful duties.

53. The legislative schemes we recommend here will also remove the temptation on the part of members of the R.C.M.P. to resort to violations of the Criminal Code in order to obtain and use appropriate cover documentation. Thus, where surveillance team members are supplied with documentation through a legislated scheme, there will be no obtaining by a false pretence, contrary to section 319 of the Criminal Code. Also, there will no longer be a need for cover documentation to be manufactured by the R.C.M.P. themselves for individuals engaged in surveillance, and there will therefore be no violations of sections 324 and 326 of the Criminal Code, dealing with forging and uttering forged documents. Similarly, there will be no need for members to personate someone else at a qualifying examination in order to obtain appropriate documentation; this resolves the problem, potential or actual, raised by section 362 of the Criminal Code. In short, selective amendments at the provincial level to what some have termed "minor" or "regulatory" laws will, with respect to these matters, eliminate the potential for violation of criminal laws in order to protect the security of Canada.

(c) *Laws relating to trespass*

54. An initially attractive solution to the trespass issue seems to lie in asking the owner of the target's apartment building, for example, for permission to enter the premises to search for the target's car. If such consent to enter is obtained, no offence is committed. While most individuals likely will grant permission to enter if the circumstances are explained to them, a real danger exists that the person's knowledge might eventually compromise the secrecy of the surveillance operation.

55. If entry into buildings and onto land is to be permitted for physical surveillance teams, it is best done with the protection of legislation. We are satisfied that the balance between property rights and the need for effective security intelligence operations favours the amendment of trespass legislation to permit entry onto land or into buildings (other than a house, or in the case of an apartment building, inhabited rooms) in order, for example, to determine the presence of an individual or of his vehicle or to plant tracking devices on the vehicle. Amendments to legislation should apply to federal and provincial police forces, as we have recommended in the section of this chapter dealing with rules of the road.

56. The legislation should be framed to provide a defence to a petty trespass prosecution where the accused is a peace officer or a person designated by the provincial attorney general and was engaged at the time of the entry in the discharge of his otherwise lawful duties and acting with due regard for the property rights of the owner. Furthermore, the trespass should be reasonably

necessary in all the circumstances. While it is hard to conceive of circumstances in which damage would occur, civil remedies against the Crown for damage occasioned in the course of such entries should continue to exist, as in the case of damages arising from automobile accidents. Again, no liability should be imposed on individual surveillance team members where they act in a fashion that entitles them to rely on the proposed defence. The federal government should compensate those individuals who suffer damages as a result of a trespass by security intelligence surveillance team members. The quantum of compensation should be assessed on the same basis as is the practice in civil courts, whether or not the civil courts or some other tribunal hear the complaint.

57. The Criminal Code offences of mischief (section 387) and damage to property (section 388) remain a problem. Increasingly effective methods of counter-surveillance necessitate considerable ingenuity on the part of individuals engaged in surveillance. To this end, surveillance operations may involve placing objects on a target vehicle. We accept the need for the use of such techniques. Therefore, we must address the problems caused by these Criminal Code offences. The only practicable solution we see is the enactment of a defence that will protect designated individuals acting in the course of their otherwise lawful duties, if they do no more damage or interfere no more with the property than is reasonably necessary for the purposes of the operation. In any event, the damage or interference should not be such as to create any danger in the use of the property. Civil recovery should be permitted according to principles similar to those enumerated in respect of rules of the road and provincial trespass legislation. This defence seems at first very broad; its ambit can be restricted considerably by limiting the number of designated individuals permitted to engage in such conduct.

WE RECOMMEND THAT, in order to make it possible for physical surveillance operations to be carried out effectively by a security intelligence agency, changes be made in federal statutes and the co-operation of the provinces be sought to make changes in provincial statutes as follows:

(1) *Rules of the road*

(a) A defence be included in provincial statutes governing rules of the road for peace officers and persons designated by the Attorney General of the Province on the advice of the Solicitor General of Canada ("designated individuals") if such persons act

(i) reasonably in all the circumstances,

(ii) with due regard for the property and personal safety of others, and

(iii) in the otherwise lawful discharge of their duties;

(b) a defence similar to that referred to in (1)(a) above be included in relevant provincial legislation which authorizes municipal traffic by-laws;

(c) there be enacted by each of the provinces and territories, a provision for the protection of peace officers and designated individuals, saving them harmless from personal liability in civil suits, if such persons act

(i) reasonably in all of the circumstances;

(ii) with due regard for the property and personal safety of others; and,

(iii) in the otherwise lawful discharge of their duties;

(d) the Government of Canada compensate those persons who, but for recommendation (c) above would be entitled to recover damages in a civil suit brought against a federally engaged peace officer or designated individual in a cause of action arising by reason of acts done or omissions occurring in the course of the work of such peace officer or designated individual and on the principle that the quantum of compensation should be assessed on the same basis as is the practice in the civil courts.

(2) *False identification*

(a) Provincial highway traffic legislation regulating the licensing and identification of persons and property be amended to permit the Director General or designated member of the security intelligence agency (or a duly authorized member of a police force) to apply for false identification to the senior government official charged with the administration of the legislation. Provision be made to permit the documents related to the application to be sealed and not to be opened without court order. It is further recommended that such amendments be made as may be necessary to remove all statutory restrictions on the signing or holding of more than one piece of identification in each case;

(b) provincial hotel registration legislation be amended to make available a defence to peace officers and designated individuals who register in a hotel under a false name provided that

(i) they do so in good faith, and

(ii) the use of a false name is necessary for the performance of their otherwise lawful duties.

(3) *Trespass*

(a) Provincial petty trespass statutes be amended to make available a defence to peace officers and designated individuals who enter onto private property other than private dwelling-houses or inhabited units in multi-unit residences but including vehicles, providing that

(i) entry onto private property is reasonably necessary in the circumstances;

(ii) they show due regard for the property rights of the owner; and,

(iii) they act in the otherwise lawful discharge of their duties.

(b) sections 387(1)(a) and 387(1)(c) and 388(1) of the Criminal Code be amended to make available a defence to peace officers and designated individuals in order to allow the attachment of tracking devices to vehicles, in order to assist in physical surveillance operations, provided that such persons

(i) act in the course of their otherwise lawful duties,

(ii) do no more damage or interference with the property than is reasonably necessary for the purposes of the operation; in any event, the damage or interference must not render the use of the property dangerous;

(c) civil remedies be preserved for both trespass and the affixing of devices in a manner similar to that recommended in respect of rules of the road. (16)

D. UNDERCOVER OPERATIVES

58. The use of human sources and undercover members, collectively referred to by us as "undercover operatives", is the most established method of collecting information about threats to security. Despite the technological revolution which has provided a variety of technical alternatives as a means of penetrating secretive organizations, the undercover operative is likely to remain an extremely important source of information to a security intelligence agency.

59. An undercover operative can be a much more penetrating means of collecting information than any technical device. A technical source — whether a hidden microphone, a telephone tap, or a long-distance viewing device — is essentially a passive instrument which can record only what is said or done at one particular place. In contrast, undercover operatives — human spies — have frequently penetrated the innermost circles of groups, probed the intentions of their leading members, and actively attempted to thwart the groups by supplying misleading information, sowing the seeds of distrust amongst their members, or otherwise disrupting the groups.

60. While there is no doubt that undercover operatives have certain advantages as sources of information, there is also no doubt that the use of these individuals by a security intelligence agency involves a number of serious hazards. Unlike information obtained from the mechanical recording of conversations, information, particularly from human sources (who, it will be recalled, are not members of the Force) must be carefully assessed for its reliability. Mechanical recording devices do not lie or exaggerate or distort; human sources can and do. The use of undercover operatives also involves the security agency in directing individuals to deceive, indeed to betray, the organizations which they penetrate. Frequent participation in the planning and execution of deceitful and treacherous acts may have deleterious effects on the moral character of the 'handlers' of these operatives and the operatives themselves. Undercover operatives may go far beyond gathering information. They might endeavour to trap the group into carrying out incriminating actions — become, in effect, *agents provocateurs* — or carry out the kinds of disruptive tactics which have come under review by us. The agency which uses undercover operatives is apt to incur serious and difficult responsibilities to protect these individuals when they are exposed or have otherwise completed their assignment.[6] Also, there are, as we indicated in Chapter 9 of Part III, a number of laws which have been violated by the use of undercover operatives.

The need for controls

61. In the past, there has been far too little attention paid to the policy and legal problems associated with the use of undercover operatives in security

[6] For an examination of the policy issues arising from the use of informants in national security investigations see the following: Christopher Felix, *A Short Course In The Secret War*, New York, E.P. Dutton, 1963, esp. Ch. III; Garry T. Marx, "Thoughts on a Neglected Category of Social Movement Participant; the Agent Provocateur and the Informant", *American Journal of Sociology*, Sept. 1974, pp. 402-442; Geoffrey Robertson, *Reluctant Judas*, London, Temple Smith, 1976.

intelligence (or, for that matter, in criminal) investigations. This is particularly true of responsible Ministers. Guidelines concerning the use of undercover operatives were developed by the Security Service but were not submitted to, nor requested to be seen by, Solicitors General. Mr. Starnes, as Director General of the Security Service, was unable to obtain a Cabinet decision on how to resolve the dilemma of the apparent need of some undercover operatives to commit offences in order to maintain their credibility with violence-prone groups.[7] The policy issues associated with the use of undercover operatives are too important to both the security of Canada and the quality of its democracy to be left entirely to investigative agencies to resolve.

62. In designing a system to control a security intelligence agency in the use of undercover operatives, a distinction must be made between those who are developed or induced to provide information and those who volunteer information or from whom information is obtained without the expectation that they will become established sources of information about a particular subject of investigative interest.[8] In our view, the use of the former type of individual who is induced by the promise of money or some favour or by political ideology, to provide information to the state about his supposed political associates, or who may be a member of the security intelligence organization temporarily living an undercover existence as a member of a targetted organization, requires a higher form of authorization and tighter method of control than the use of sources on a voluntary or occasional basis. Hence in the system of controlling the general level of investigation which we proposed above, ministerial authorization would be required for any investigations involving "developed human sources" and members operating undercover.

63. We realize that the distinction between 'developed' and 'undeveloped' human sources will not always be easy to make. After all, the use of undercover operatives involves human relationships whose essential characteristics are not as self-evident as those of mechanical devices. Still, in the vast majority of situations we think it should be reasonably clear whether or not a person is being cultivated as a continuing long-term source of information about a particular organization. But here again, we should note that, if the members of the security organization have no understanding of or respect for the principle at stake in distinguishing between the different types of undercover operatives and in requiring a stricter method of controlling the most intrusive type, then the system of control will be frequently by-passed.

64. Evidence of growing concern about the risks inherent in the use of human sources in particular is afforded by the fact that the governments of both Great Britain and the United States have in recent years established administrative guidelines governing the use of informants by investigative agencies. In England, the Home Office has issued an administrative circular on the subject[9] and

---

[7] We deal with this matter in detail in a subsequent Report.

[8] For a description of the different types of informants used by the R.C.M.P. Security Service, see Part III, Chapter 9, section A.

[9] *Home Office Consolidated Circular to the Police on Crime and Kindred Matters.*

in the United States, Attorney General Levi established guidelines for the F.B.I.'s use of informants.[10] The latter are more pertinent to our concern in this chapter as they pertain to the F.B.I.'s domestic security investigations whereas the British directive pertains to criminal investigations. The introduction to the F.B.I. guidelines states that "while it is proper for the F.B.I. to use informants in appropriate investigations, it is imperative that special care be taken not only to minimize their use but also to ensure that individual rights are not infringed and that the government itself does not become a violator of the law". In using informants for authorized investigations the guidelines require the F.B.I. to consider a number of factors, the first of which is

> The risk that use of an informant in a particular investigation or the conduct of a particular informant may, contrary to instructions, violate individual rights, intrude upon privileged communications, unlawfully inhibit the free association of individuals or the expression of ideas, or compromise in any way the investigation or subsequent prosecution.[11]

65. The tendency of undercover operatives to inhibit political association and dissent is particularly great in security intelligence investigations where the groups which are subject to investigation are, by definition, political. Excessive planting of secret state operatives in political organizations could have, to use the language of American Constitutional law, "a chilling effect" on the exercise of freedom of speech and freedom of association in Canada.[12] These values, which are now recognized as fundamental human rights by the Canadian Bill of Rights and Bills of Rights adopted by several of the Provinces, may in the future be entrenched in the Canadian Constitution. It is consonant with a proper concern for the effect of the use of informants on fundamental political rights that we have proposed to restrict "full" investigations, including the use of developed human sources and members undercover, to situations where there is reason to believe a group is participating in espionage, sabotage, foreign interference, serious political violence or terrorism. Adoption of this proposal would mean that undercover operations could not be targetted against groups whose subversive activity went no further than the rhetorical and written espousal of revolutionary ideas.

66. Given the very serious impact which the misuse of undercover operatives can have on civil liberties and our principle that the more intrusive the technique of information collection the higher should be the authority permitting its use, it might be asked why we are not recommending that judicial authorization be required for the use of undercover operatives. We are recommending a system of judicial warrants following approval by a committee of senior officials and the Solicitor General for the use of electronic surveil-

---

[10] *Attorney General's Guidelines for F.B.I. Use of Informants in Domestic Security, Organized Crime and Other Criminal Investigations*, 1976, section 15.

[11] *Ibid.*, section A(1).

[12] Some court decisions in the United States have held that the use of undercover agents and informants in certain situations may violate the guarantees of free speech and association in the First Amendment of the U.S. Constitution; see, for example *U.S.* v. *White* 120 Cal. Rptr. (1975) 94, 533 5.2d 222 and *Local 309* v. *Gates*, (1948), 75 F.Supp. 620 (N.D. Ind.).

lance, surreptitious entry, mail opening, and access to personal information beyond biographical information on government files. Why not also require judicial warrants for the use of undercover operatives? We rejected a requirement of judicial warrants for the more intrusive type of operative for two reasons. First, there is an unavoidable lack of precision in identifying those individuals whose use requires the approval of higher authority and those whose use does not. As we have stated, obtaining information through undercover operatives involves human relationships whose defining characteristics are more complex than those of mechanical devices. Second, we think that requiring a judicial warrant for an investigative technique as subtle and complex as the use of undercover operatives is apt to involve the judiciary too closely in the investigative process. We note that Attorney General Levi advanced a similar argument in explaining to a congressional committee in the United States his decision not to require judicial warrants for the use of informants in domestic security investigations:

> Extending the warrant requirement in this way would be a major step towards an alteration in the basic nature of the criminal justice system in America... It would be a step toward the inquisitional system in which judges, and not members of the executive, actually control the investigation of crimes. This is the system used in some European countries and elsewhere, but our system of justice keeps the investigation and prosecution of crime separate from the adjudication of criminal charges. The separation is important to the neutrality of the judiciary, a neutrality which our system takes pains to protect... We must ask ourselves whether the control of human sources of information — which involves subtle, day-to-day judgments about credibility and personality — is something judges ought to be asked to undertake. It would place an enormous responsibility upon courts which either would be handled perfunctorily or, if handled with care, would place tremendous burden of work on federal judges.[13]

The need for ministerial guidelines

67. In addition to the system of prior approval for the use of undercover operatives which we have recommended in section B of this chapter, we think that a set of guidelines approved by the Solicitor General should be developed on important policy issues which arise in the use of undercover operatives. A section of the R.C.M.P. Security Service Operations Manual deals with a number of the subjects that should be covered in such guidelines, but the manual itself has not been subject to ministerial approval. Once they are approved the guidelines should be publicly disclosed, although they need not contain information about operational techniques, the disclosure of which would endanger the security of operations. They should express the principles which govern the use of human sources and members undercover by the security agency — principles which should be open to public scrutiny.

68. Throughout this Report we have referred to various forms in which policy direction is issued by the R.C.M.P. Words used by the R.C.M.P. to describe

[13] Quoted in John T. Elliff, *The Reform of F.B.I. Intelligence Operations*, Princeton, Princeton University Press, 1979, p. 126.

these different forms include "directives", "bulletins", "policy", "guidelines", and "manuals". Further, some of these words are, on different occasions, used in different senses. The consequence appears to be that there is no clear and consistent understanding by those who receive the policy direction as to their obligation to comply with it. This was exemplified to us in the testimony of a senior officer who told us that he regarded the then existing policy prohibiting telephone tapping as a "guideline" but that he also considered it to be a "policy" and "to some extent" a "binding rule". On the other hand, according to his testimony, even though he considered it as a "policy", there had to be room for "discretion and the exercise of judgment" in the application of the policy (Vol. 34, pp. 5506-9). Another illustration of the problem arises in Bulletin OM-82. We discussed the contents of that bulletin in Part III, Chapter 8. That bulletin was issued by the Commissioner in 1980 to become a part of the Operational Manual of the Force. It contained a statement that "The following general guidelines must therefore be adhered to in future". The Commissioner has advised us that, notwithstanding his use of the imperative word "must" in the bulletin, he did not intend it to be an "order", with the exception of the part that indicated that all members are expected to comply with provincial statutes and municipal bylaws in relation to traffic. He says that the remainder of the bulletin is "only a guideline". We are very concerned about the uncertainty that apparently surrounds the meaning and effect of the different words used by those promulgating policy direction. We think it probable that members in the field have the same difficulty we have encountered in knowing how "binding" a "policy" or a "guideline" or a "bulletin" is, and therefore in anticipating what the consequences may be if they do what the document says should not be done or fail to do what the document says shall be done. It is important that members receive more guidance than a simple assurance that their conduct, if reasonable, will not be judged adversely. Of equal importance to the members having a clear understanding of what the consequence of a breach of policy direction will be is that there be a systematic and critical scrutiny of the interpretation and practical application of the policy directions which are issued. Such a review and scrutiny must take place both within the police force and the security intelligence agency and also outside of them. So that such review and scrutiny can be made outside, the Minister responsible should be advised of all policy directions issued by the Commissioner of the R.C.M.P. or the Director General of the security intelligence agency — whether they are called "policy", "guidelines", "directives", "bulletins", or "manuals". In this Report we frequently recommend that the Minister responsible for the security intelligence agency should issue guidelines to the agency. We are conscious that the word "guidelines" may be used in several senses, including a mandatory sense and a discretionary sense. It is important that members of the agency know whether a guideline is mandatory or discretionary, that problems of interpretation in the field be drawn to the attention of the management of the agency, and that the interpretation and application of the guidelines be the subject of continuing scrutiny by the Minister, the Deputy Minister, the Director General, and the Advisory Committee on Security and Intelligence.

69. In the paragraphs that follow we discuss those matters relating to the use of undercover operatives which have raised legal or policy issues in the past and should be dealt with by administrative guidelines approved by the Solicitor General and in some cases also by legislative amendment.

The use of deceit

70. The recruitment and use of undercover sources necessarily involve deceitful activities. Recruiting a member of a foreign intelligence agency or a terrorist group to become a source of information for Canada's security intelligence agency entails inducing an individual to commit an act of betrayal and to deceive his present associates. Penetration of a group threatening security by a member or agent of the security intelligence agency can be accomplished only through falsifying the member's or agent's true identity and purpose. While we recognize the inevitability of deceit in the tradecraft of a security intelligence agency, we think there are limits beyond which deceitful activity must not be permitted to go. One limit, which we have already insisted upon, is that the source's activities must be lawful. Another is that the security intelligence agency must not deceive Ministers or senior government officials, nor should it falsely allege that a Minister has given an undertaking to protect or assist an informant. The ministerial guidelines on undercover operatives should clearly identify the forms of deceit which are unacceptable.

Lawfulness of operative's activity

71. Throughout this Report we have taken the position that there must be no departures from the rule of law in the policies and practices of a security intelligence agency. That principle should certainly be applied to the use of undercover operatives — whether the individual is an undercover member of the security agency or a person outside the organization acting as a source. We do not think there should be a double standard of acceptable conduct. Ensuring both the lawfulness and effectiveness of undercover operatives will, as we indicated in Part III, Chapter 9, require some legislative amendments. First, the need for false documentation to hide the true identity of the undercover operative (normally a member undercover) will require changes in federal and provincial laws similar to those proposed in relation to physical surveillance. In addition to provisions in laws relating to motor vehicle registration, driver's licences and hotel registration, provision should also be made where necessary for obtaining false documentation in laws governing S.I.N. cards, passports, birth certificates and education certificates. This would alleviate the need to manufacture and obtain documentation in a manner that in the past has resulted or may have resulted in violations of the Criminal Code: section 320 (obtaining by false pretences); sections 324 and 326 (forging and uttering forged documents); section 335 (offences in relation to register); and, section 362 (personation at an examination). Secondly, federal and provincial tax legislation should be amended to permit security intelligence agency sources not to declare as income payments received by them from the agency. We arrived at this position after considering and rejecting the feasibility of a system that would deduct tax payments from the payments to the source. (For

example, it would be next to impossible to determine accurately the rate at which such payments should be taxed.) We think this legislative amendment is needed to protect the identity of sources and to avoid a situation in which members of the security intelligence agency advise paid sources not to declare their payments as taxable income and thus conspire with their sources to break the provisions of the Income Tax Act. Further, the government should ascertain whether there are other legislative requirements governing employer and employee relations which may relate to payment of human sources, compliance with which would result in disclosing the identity of the source, and should seek whatever amendments may be necessary to overcome these difficulties.

72. A third area in which legislative reform is needed if sources are to be used effectively and lawfully for security intelligence (or criminal intelligence) purposes is section 383 of the Criminal Code which is concerned with secret commissions. As our analysis in Part III, Chapter 9, pointed out, judicial construction of this section necessitates an amendment to provide expressly that neither an agent nor an employee commits an offence in providing information about a principal or employer if this is done in the course of an authorized security intelligence investigation. In addition to this legislative change the guidelines governing the use of undercover operatives should recognize the need to balance the damage to the relationship of trust between employer and employee or principal and agent which use of a source may entail, against the potential value of the information for the protection of national security.

73. There is one further change in the law to which we have given careful consideration. That is whether there should be provision in law to allow security intelligence agency undercover operatives to perform acts which would otherwise be offences in order to establish or maintain their credibility with the groups they are attempting to penetrate. The R.C.M.P. Security Service raised this issue in relation to problems encountered in penetrating Quebec terrorist groups in the late 1960s and early 1970s. As we reported in Part III, Chapter 9, we have reviewed the extent to which the operational branches currently identify a need for undercover operatives to commit offences to maintain credibility. While the current operational policies of the Security Service prohibit instructing a source to commit an offence, they appear to leave the door open for a source to become involved in a criminal offence by stating that

> The D.D.G. [i.e. the Deputy Director General] has ruled that *any* degree of source involvement in *any* premeditated criminal offence will be decided by Headquarters on the events of each particular case. The support of the A/Gs or other appropriate authority, will have a definite bearing on such decisions.

74. We consider that the existing policy is unsatisfactory. Premeditated criminal offences by security intelligence undercover operatives must not be permitted under any circumstances. We considered two possible changes in the law which would provide greater leeway for security intelligence informants:

(1) A statutory defence for the commission of certain offences.

(2) A system of prior approval whereby in clearly defined circumstances and under appropriate controls an undercover operative of the security agency could be authorized to carry out a range of acts which would otherwise be offences.

We have concluded that there is not sufficient need to change the law in either of these ways. In taking this position we acknowledge that there will likely be situations in which sources or members of the security intelligence agency will have to forfeit their credibility with targetted groups and their usefulness as undercover operatives in order to avoid unlawful activity. This policy means that the security intelligence agency's informants will not be able to penetrate cells of movements in which the commission of an offence is the passport to admission, and will find it difficult, and in some cases may find it impossible, to play any role in violence-prone groups. But neither our extensive review of Security Service experience to date nor our speculation about future security threats, especially the threat of terrorism, has convinced us that the 'evil' to be thwarted is great enough to justify the 'evil' of secretly authorizing agents of the government to carry out a range of activities which would otherwise constitute criminal conduct, no matter how carefully and narrowly the criteria are drawn. The fact that the magnitude or urgency of future threats to security is unpredictable does not in our view justify stretching so ominously the leeway available under law to the agents of national security. Our conviction that the law should not be amended to expand the scope of lawful conduct by security informants is strengthened by recognition of legal mechanisms already available. The common law defences of necessity or duress might be of assistance to an operative in circumstances where the carrying out of an act which might otherwise be an offence appears to be the only means of avoiding serious bodily harm. Further, discretion in prosecuting and sentencing, as well as the prerogative power of mercy, may all be exercised in favour of a person whose criminal conduct can be shown to have been carried out for the purpose of protecting national security. The policy of the security intelligence agency should prohibit civil wrongs, as it would other unlawful conduct, on the part of undercover operatives. Nevertheless, there may be circumstances when such torts as we examined in Part III, Chapter 9 — inducement to breach of contract and invasion of privacy — may occur as the result of the activities of undercover operatives. If that should happen, and if individuals have suffered loss or damage as a result, the Crown should make *ex gratia* payments to them to compensate them.

75. The alternative to the position we have taken is to change the law so that under certain circumstances undercover operatives of the security intelligence agency could lawfully engage in conduct which would otherwise constitute criminal activity. This alternative could take the form of a provision in the Act governing the security intelligence agency whereby, under exceptional circumstances when the conduct is necessary to obtain information about a serious threat to security, a Committee of Ministers could, in advance, authorize the agency to permit certain of its members or sources to participate in conduct which would otherwise constitute a criminal offence. Such a provision could stipulate a limited range of permissible conduct that might well exclude either

bodily harm to persons or serious damage to property. The undercover operative of the security intelligence agency who engaged in such conduct would then not be committing an offence so long as the conduct was properly authorized and within the range of activity described in the Act. We have rejected this alternative and opted for the status quo because we think such an extension of investigative powers involves encroachment on civil liberty that would be a more serious evil than the damage to security resulting from the fact that the security intelligence agency lacks these powers. We realize that the position we have taken involves a certain risk that threats to security will go undetected. We also note that, in the United States, Guidelines governing F.B.I. investigations signed by Attorney General Civiletti on December 2, 1980[14] authorize "otherwise criminal" activity by F.B.I. informants under specified circumstances and subject to a prescribed approval process. These guidelines apply to both the domestic security and criminal investigation activities of the F.B.I. Because of the risk to security which our approach entails, we think that, if this approach were to be followed by the Government of Canada, its consequences should be carefully reviewed by the government and by the Special Parliamentary Committee on Security and Intelligence within 5 years. This review should attempt to adduce whatever evidence there is of damage to Canada's security resulting from the absence of any power on the part of security intelligence agency informants to commit "otherwise criminal" activity. This review should also examine as thoroughly as possible the experience of the United States and other western democracies that have adopted arrangements to authorize "otherwise criminal" activity by security informants.

Reporting unlawful acts of undercover operatives

76. Despite the policies and clear instructions of the security agency, an undercover operative might participate in criminal activity in the course of carrying out an assignment for the agency. Or the human source might participate in criminal activity unrelated to his work for the agency. Normally, in either case, the agency should report whatever knowledge it has of criminal activity to the law enforcement agency which has jurisdiction to investigate the activity in question. However, there may be situations in which the agency believes that the information an operative may obtain is of such importance to the protection of national security that information about the source's criminal activity should not immediately be turned over to law enforcement authorities. In situations of this kind where the requirements of law enforcement must be balanced against the needs of national security, the security agency must not be left on its own to determine which consideration should be given priority. When the agency thinks that the withholding of information about unlawful conduct of its sources is justified it should notify the Attorney General of Canada, who should be responsible for deciding whether or not the information

[14] *Attorney General's Guidelines on F.B.I. use of informants and confidential sources* (under the authority of the Attorney General as provided in 28 U.S.C. 509, 510, 533), Office of Attorney General, Washington, D.C., December 12, 1980.

should be turned over to the appropriate law enforcement authorities, according to arrangements we shall describe in Chapter 8 of this Part.

Disruptive activities by undercover operatives

77. As we reported in Part III, the Security Service sometimes has used undercover operatives as much for the purpose of disrupting or breaking up organizations as for the purpose of collecting information about them. In Chapter 6 of this part of our Report we shall set out our recommendations with regard to this type of disruptive activity: here we should note that the main recommendation we shall make — namely, that such activity should not be permitted outside of counter-espionage and counter-intelligence operations — should be incorporated in the guidelines governing the use of undercover operatives. Another kind of activity closely related to attempts by operatives to disrupt organizations consists of attempts to trap individuals in situations which will lead to their prosecution by provoking or instigating their participation in criminal activity. Because such attempts at entrapment or the activities of *agents provocateurs* are likely to occur more often in criminal investigations directed towards obtaining evidence to support a prosecution than in security intelligence investigations, we will deal with this problem in Part X, Chapter 5, where we consider legal reforms related to the criminal investigation responsibilities of the R.C.M.P. But aside from any changes which may be made in the Criminal Code to bar the use of evidence obtained in this way, the policy guidelines governing the use of undercover operatives should prohibit these individuals from instigating or encouraging unlawful conduct. Further, undercover operatives should be instructed to do what they can to influence groups who may be planning acts of violence to adopt milder methods of protest.

Pretext interviews

78. The security intelligence agency should not use the interviewing of a candidate for security clearance as an occasion for recruiting that person as a source. Such an abuse of the agency's security screening responsibilities is one which is most likely to occur in immigration and citizenship screening. It can have the unfortunate effect of making it appear to the applicant that he or she must agree to become an established source of information to the security agency as a condition for obtaining clearance. There may be circumstances in which a person interviewed in the course of security clearance proceedings appears to be an important source of information about a security threat which is currently under investigation. In those circumstances, if such a person is to be used as a source, the approach to him for recruitment purposes should not be made during the screening interview. The timing of the approach should be such that there is no possibility that the person will feel that he is being coerced into becoming a source. Preferably the approach should be made after the security screening decision has been made and communicated to him.

Undercover operatives and the integrity of certain institutions

79. There can be no doubt that the excessive or thoughtless use of security intelligence sources in certain contexts can have a very adverse effect on

institutions which are vitally important to our liberal democratic society. The current policy that requires ministerial approval for the use of paid sources who are to be used by the Security Service to gather intelligence solely on a university or college campus gives limited recognition to this point. Certainly the free flow of ideas and the freedom of inquiry so essential to the institutions of higher learning in a free society would be seriously threatened by the widespread planting of undercover operatives in colleges and universities. But colleges and universities are by no means unique in this respect. For example, the ability of journalists to obtain information essential to the functioning of an effective free press may be damaged if it is known or believed that journalists are widely used as security intelligence sources. Or, to take another sector of society, freedom of worship and religion may be adversely affected if priests or other religious functionaries are frequently employed to spy. The problem here is not only a source problem; it is a problem with undercover members who might seek to pose as teachers, journalists etc. The chilling effect is the same.

80. The threat posed to the integrity of institutions by the use of undercover intelligence agents has received considerable attention in the United States. The Senate Select Committee to Study Governmental Operations with respect to Intelligence Activities (the Church Committee) focussed attention on the risks associated with the use of academics, members of the media and of religious organizations as undercover informants. Draft legislation based on the Church Committee Report contains provisions prohibiting the use of membership in religious, media or educational organizations as a cover for an officer of an intelligence agency.[15] In Canada, only academic institutions have been specifically singled out in policy instruction as requiring particular sensitivity and control in relation to the use of sources. Mr. Dare indicated in his evidence before us that there is no policy with respect to other kinds of institutions beyond "the good common sense of very seasoned people..." (Vol. 318, p. 301693).

81. In our view the list of valuable institutions whose effective functioning may be adversely affected by the activities of undercover operatives extends far beyond academic institutions, the media and religious organizations. Labour unions and business corporations, cultural and ethnic organizations, for example, all of which play a valued role in our society, may also be adversely affected. Therefore, we think the guidelines governing the use of undercover operatives should reflect a general sensitivity to the damage which undercover operatives may do to all legitimate social, economic and political institutions. We think that sensitivity of this kind, exercised by security intelligence operatives in carrying out such investigations governed by the system of controls we have recommended, is preferable, as a basis for sound practice, to rules developed for specific areas such as those which now govern Security Service activity on university campuses. However, we acknowledge that the sensitivity required will not likely exist unless the recruitment and training of security intelligence officers are changed along the lines we shall recommend later.

---

[15] See *National Intelligence Reorganization and Reform Act of 1978 — s.2525* (The Huddleston Bill), s.132.

82. In calling for the security intelligence agency to exercise sensitivity to the integrity of valued institutions in using undercover operatives, we should, at the same time, recall a fundamental point we made in the earlier chapter on the scope of security intelligence surveillance — namely that no sector of society should be treated as immune to security intelligence investigations.

Confidential relationships

83. The use of human sources by a security intelligence agency may encroach upon confidential relationships in the private sector or between the citizen and government. For instance, the agency may wish to obtain information from lawyers or doctors about their clients or patients or from government officials who have access to personal data of a confidential nature.

84. As far as the private sector is concerned, as we reported in Part III, a security intelligence agency will come up against a number of legal difficulties when dealing with sources who are members of professional groups obliged to respect the confidentiality of certain kinds of information. The law of contract and tort may also create difficulties in the commercial sector. However, our assessment of the security agency's need for information did not convince us that the law needs to be amended (or clarified) to remove possible legal barriers to the security intelligence agency's use of sources in the private sector. There is one qualification we must make to this finding, pertaining to members of the medical profession. In preparing this Report we anticipated not being able to comment on such sources because we wished to wait until the report of the Ontario Commission of Inquiry into the Confidentiality of Health Information[16] (the Krever Commission) was available. That report has just recently become available and we have chosen to comment in one place on the several respects in which it touches upon matters of concern to us. Those comments are found in Annex I at the end of this Report.

85. The position we have taken with regard to the use of sources in the private sector who may be required by law not to provide certain kinds of information means that the security intelligence agency must have the assistance of a well-qualified legal adviser. The security agency must not violate legally protected confidential relationships in its use of sources. In determining whether or not legal difficulties exist, the security agency must not be guided by amateur and simplistic assessments of these difficulties. The law in this area is complex and dynamic, and the need for experienced and highly qualified legal advice is one of the reasons for our recommendation, in Part VI, for a Legal Adviser.

86. Turning now to the public sector, we think it is wrong for the security intelligence agency to use undercover sources in government departments to obtain confidential government information. The Security Service is now legally barred from obtaining access to certain kinds of biographical and personal information in federal government information banks which we think

---

[16] *Report of the Commission of Inquiry into the Confidentiality of Health Information*, Toronto, 1980.

it should have for authorized security investigations. In section H below, dealing with access to confidential information, we shall recommend certain changes in federal law to facilitate the access which we believe is required. Section 8(2) of the government's proposed Privacy Act (Schedule II of Bill C-43 which had its first reading on July 17, 1980) could permit access to confidential personal information:

> (e) to an investigative body specified in the regulations, on the written request of the body, for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation, if the request specifies the purpose and describes the information disclosed;
>
> (l) for any purpose where, in the opinion of the head of the institution,
>
> (i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure.

It should be noted that in relation to subsection (l), the R.C.M.P. is designated, for purposes of the Act, as a "government institution". The government's proposed legislation on this subject would establish means of access for a security intelligence agency to personal information held by federal government departments and agencies. Our own proposals set out a more exacting system of control and review. This is the only way in which a security intelligence agency should gain access to confidential personal information in the possession of the federal government.

87. The policy which we recommend as appropriate for obtaining information from federal government departments and agencies should also apply to obtaining information from provincial and municipal governments. The security intelligence agency should not develop undercover sources within provincial or municipal governments as a means of obtaining access to information held by these governments. In Part III, Chapter 9, we reviewed provincial laws which govern access to information used in past operations by the Security Service. With the exception of hospital and health insurance records, on which we shall comment in Annex I, where we examine the relevant recommendations of the Krever Commission, we have concluded that there is no need to seek the co-operation of the provinces in obtaining amendments to laws protecting particular kinds of information. Nor do we think there is any need to seek exemptions from secrecy provisions of general application. In most cases, such as the civil servant's oath of secrecy, where government information is protected by general secrecy provisions, there is a convention that a Minister or head of department or agency has a discretionary power to disclose information. The proper course of conduct for a security intelligence agency which wishes access to such information is to request it from the Minister or official who is authorized to release the information.

88. We realize that a policy of confining the security agency's access to provincial or municipal government information to what can be obtained lawfully through authorized channels of communication precludes 'targetting' a provincial government which is suspected of supporting or participating in activity threatening the security of Canada. This would rule out, for instance, using a member of a provincial government as a source of information about

that government's suspected involvement in clandestine foreign interference in Canadian political life. As we pointed out in Part III, a municipal or provincial official who 'spies' on the government which employs him, may, among other things, violate section 111 of the Criminal Code which defines the offence of breach of trust by a public officer. But aside from legal prohibitions, we think it bad policy in a federal state for one level of government to spy on the other. While federal and provincial governments have had serious differences, including differences about Canada's constitutional future, these differences have not been about the fundamental importance of maintaining the democratic process of government, the protection of which is the ultimate purpose of national security arrangements. We think it would be unreasonably pessimistic to foresee a change in that situation sufficient to justify amending the laws of Canada to permit a national security intelligence agency to use undercover sources within provincial or municipal governments.

The distinctiveness of security intelligence sources

89. We have found that the effectiveness of a security intelligence agency may be adversely affected if in its treatment of long-term undercover sources it is too closely influenced by attitudes that policemen usually have to "informers". Policemen do not hold such persons in high regard. They tend to think of informers in the drug world, for example, in much the same way as they do criminals. Consequently a policeman finds it very difficult to understand that a long-term agent in place, such as a member of a political group who reports to the Security Service regularly on the activities of the group, is a different kind of person. He finds it hard to undertand that many such sources have originally volunteered to help the R.C.M.P. not because of a prospect of payment of money but because of their own concern that the activities of the group, or of some members of the group, are inimical to the interests of Canada. He finds it hard to understand that many such sources continue to lead their double life, sometimes at continuing risk of personal danger, and frequently at the expense of their own normal vocational development and personal life, not solely because of what money they are paid but because of a moral commitment to serve Canada. That motivation often *is* present. Yet it was reported to us that in 1980 a very senior officer in the R.C.M.P., all of whose experience had been on the criminal investigations side of the Force, when addressing a large group of members of the Security Service, spoke of some human sources in extremely derogatory terms. Nothing could have demonstrated more clearly to his audience that he and others like him, with criminal investigation backgrounds, were unlikely ever to be able to understand the handling of security intelligence sources, perhaps the most difficult aspect of investigative work, by a security service.

WE RECOMMEND the establishment of administrative guidelines concerning the principles to be applied in the use of undercover operatives by the security intelligence agency. These guidelines should be approved by the Solicitor General, as the Minister responsible for the security intelligence agency and should be publicly disclosed. These guidelines should cover, *inter alia*, the following points:

(a) the forms of deceit which are unacceptable;

(b) sources and undercover members must be instructed not to participate in unlawful activity. If an undercover operative finds himself in a situation where the commission of a crime is imminent, he must disassociate himself, even at the risk of ending his involvement in the operation. In situations where there is time to seek advice as to the legality of a certain act required of the undercover operative, such advice should be sought. If the act is considered to be unlawful, alternative courses of action should be considered. In many situations, this will allow the operative to continue in his role while remaining within the law;

(c) undercover operatives should not be used in situations where it is likely that the operative will be required to participate in unlawful conduct in order to establish or maintain his credibility;

(d) the agency should report unlawful conduct by undercover operatives, in accordance with the procedures which we propose in Chapter 8 of this Part;

(e) undercover operatives must not be used for the purpose of disrupting domestic groups unless there is reason to believe such a group is involved in espionage, sabotage or foreign interference;

(f) undercover operatives should be instructed not to act as *agent provocateurs* and, in situations where they become aware of plans for violent activity, to do what they can to persuade the members of a group to adopt milder methods of protest;

(g) interviews of persons for security screening purposes should not be used as occasions for recruiting such persons as sources;

(h) great care should be taken in authorizing the use of undercover operatives to balance the potential harm to which the deployment of such individuals within a social institution may do to that institution against the value of the information which may be obtained;

(i) the security intelligence agency should respect confidential professional relationships and other legal barriers to the use of sources in the private sector and should be directed by expert legal advice as to the extent of such legal barriers;

(j) employees or persons under contract to the federal, provincial or municipal governments must not be used as undercover sources in regard to matters involving their government. Confidential information held by governments must be obtained through legally authorized channels; and

(k) the making of *ex gratia* payments for loss or damage suffered as a result of civil wrongs committed by undercover operatives. (17)

WE RECOMMEND THAT to facilitate the obtaining of false identification documents in a lawful manner for undercover agents of the security intelligence agency, federal legislation be amended, and the co-operation of the provinces be sought in amending relevant provincial laws, in a manner similar to that recommended for the false identification needed in physical surveillance operations. (18)

WE RECOMMEND THAT income tax legislation be amended to permit the security intelligence agency sources not to declare as income payments

received by them from the agency, and that other fiscal legislation requiring deduction and remittance by or on behalf of employees be amended to exclude such sources.

(19)

WE RECOMMEND THAT section 383 of the Criminal Code of Canada concerning Secret Commissions be amended to provide that a person providing information to the security intelligence agency in a duly authorized investigation does not commit the offence defined in that section.

(20)

E. ELECTRONIC SURVEILLANCE

90. The interception of oral communications by technical devices is an important means of collecting information about activities threatening the security of Canada. This method of collecting information takes two different forms: the recording of telephone conversations ('wire taps') and the planting of hidden microphones ('bugging'). We have reviewed the use of these techniques by the R.C.M.P. Security Service, especially since 1974 when the use of electronic surveillance became subject to the terms of section 16 of the Official Secrets Act. This review has left no doubt in our minds as to the necessity of using electronic surveillance for the protection of national security. There are groups and organizations in the espionage, foreign intelligence and terrorist fields that are very difficult to penetrate by human sources. In numerous situations it is reasonable to believe that such groups or organizations constitute such a serious threat to the security of Canada that advance warning is needed of their intentions and plans. Moreover, this advance warning is needed before evidence of a particular criminal activity is available. Electronic surveillance will often be the only effective means of obtaining the information which the state ought to have in these situations.

91. However, while we have no doubt as to the necessity for electronic surveillance as a technique of collecting information, we have found a number of inadequacies in the law and procedures which now govern the use of electronic surveillance by the R.C.M.P. Security Service. We identified some of these inadequacies in Part III in our discussion of practices not authorized or provided for by law. Here we shall bring together those legal considerations with other matters of policy as a basis for recommending changes in these laws and procedures.

Applications for warrants

92. Under existing procedures, proposals of field units to use electronic surveillance are reviewed at Security Service Headquarters. This review includes obtaining an opinion from a lawyer from the Department of Justice as to whether the proposed target of electronic surveillance falls within one of the categories of subversive activities listed in section 16(3) of the Official Secrets Act. If Headquarters approval is obtained, an application is prepared for a ministerial warrant. The Director General of the Security Service then presents the application to the Solicitor General, often with an aide-mémoire setting out further details with regard to the application. The Director General swears to

the truth of the information contained in the application. Normally no one else has been present when the Director General presents the application to the Solicitor General, although often the Deputy Solicitor General and the Commissioner have been present in the same room but have not participated in any way in the application. Typically requests for warrants have been put to the Solicitor General just after the weekly meetings with the Commissioner and other senior members of the R.C.M.P.

93. We are satisfied that the Security Service at Headquarters has made a conscientious effort to review the merits of proposals by field units that an application be made to the Solicitor General for a warrant under section 16. The following statistics were provided to the Commission by the section responsible for the administration of applications for such warrants, and cover the period from July 1, 1974 to August 1, 1978: 55 requests from the field for such warrants were rejected by various levels at Headquarters. Seven of those, which were rejected initially, received favourable consideration upon re-application by the field units and the provision of additional information. Also, it is evident that the several Solicitors General did not comply with all requests for warrants made by the Security Service. Eleven applications made to the Solicitors General from 1974 to 1978 inclusive were refused. In several of these instances a warrant was subsequently granted when additional information was provided.

94. There are, however, a number of improvements which we think should be made in the procedure followed in applying and granting warrants. To begin with, the 'application' — the document sworn by the Director General — has often been very brief in describing the activities of the targetted person or organization. Frequently much of the detailed information advanced in support of the application was set out in an aide-mémoire which was not formally part of the application. Mr. Dare testified that he did not consider that he was swearing to the truth of the information in the aide-mémoire. We do not think that this is an acceptable way of complying with the statutory requirement that the Minister be "satisfied by evidence on oath" of the necessity of granting the warrant. The truth of all of the evidence advanced in support of the request for the warrant should be sworn to under oath. If there are important matters of evidence which the Director General cannot in good conscience personally attest to, he should bring with him members of the security agency who can, or their sworn affidavits.

95. In considering the merits of a proposal to use electronic surveillance for national security purposes, the Solicitor General should have more advice than is now available from officials of his Department who are not members of the security agency. Under the system we have proposed for approving full investigations (in which electronic surveillance is one possible investigative technique) a senior official from the Solicitor General's Department (most likely the Assistant Deputy Solicitor General for police and security) would be included in the committee which decides whether to request ministerial authorization for a full investigation. This same official should also be involved in assessing the case for using electronic surveillance. In addition we think the Deputy Solicitor General should not be excluded from the process of appraising

applications for warrants. We note that in Great Britain every application by the Security Service for a warrant to intercept communications is submitted to the Permanent Under Secretary of State at the Home Office "who, if he is satisfied that the application meets the required criteria, submits it to the Secretary of State for approval and signature of a warrant".[17] We think it would be simpler to have the Deputy Solicitor General present when the Director General of the Security Service presents a proposal for electronic surveillance. However, whether the Deputy Solicitor General approves applications before they are submitted to the Solicitor General or is present when the Solicitor General is considering an application, the essential point is to make sure that the Minister has the advice of the most senior and experienced officials of his Department in making such a decision. It is especially important for a new Minister in his first days of office to have the assistance of a reasonably experienced Deputy, who is not a member of the intelligence agency, in assessing applications for electronic surveillance.

96. We turn now to a more far-reaching proposal for change in the existing law and procedure. We think that the use of electronic surveillance for national security purposes should be based on a clearer and more precise standard of necessity, similar to the standard established in section 178.13 of the Criminal Code for the use of electronic surveillance in the investigation of crimes. Further we believe that a judge, rather than a Minister, should make the final determination of whether a particular application satisfies the statutory conditions.

97. The conditions under which electronic surveillance may be authorized for national security purposes are now defined in section 16 of the Official Secrets Act as follows:

> (2) The Solicitor General of Canada may issue a warrant authorizing the interception or seizure of any communication if he is satisfied by evidence on oath that such interception or seizure is necessary for the prevention or detection of subversive activity directed against Canada or detrimental to the security of Canada or is necessary for the purpose of gathering foreign intelligence information essential to the security of Canada.
>
> (3) For the purposes of subsection (2), "subversive activity" means
>
> (a) espionage or sabotage;
>
> (b) foreign intelligence activities directed toward gathering intelligence information relating to Canada;
>
> (c) activities directed toward accomplishing governmental change within Canada or elsewhere by force or violence or any criminal means;
>
> (d) activities by a foreign power directed toward actual or potential attack or other hostile acts against Canada; or
>
> (e) activities of a foreign terrorist group directed toward the commission of terrorist acts in or against Canada.

[17] Cmnd. 7873, April 1980.

It should be noted that subsection (2) establishes three different tests for the issuance of warrants. The Solicitor General may issue a warrant if he is satisfied by evidence on oath that one of the following facts exists:

— that such interception is necessary for the prevention or detection of subversive activity directed against Canada;

— that such interception is necessary for the prevention or detection of subversive activity detrimental to the security of Canada;

— that such interception is necessary for the purpose of gathering foreign intelligence information essential to the security of Canada.

However, apparently little attention is given to identifying which of the three tests has been satisfied by the evidence sworn by the Director General under oath. The practice has been for the warrant to blend together all three tests and simply recite that the Solicitor General is

> satisfied by evidence on oath of Michael R. Dare, a member of the Royal Canadian Mounted Police, that it is necessary for the prevention or detection of subversive activity directed against Canada or detrimental to the security of Canada or is necessary for the purpose of gathering foreign intelligence information essential to the security of Canada to intercept and/or seize any communication hereinafter described. . .

Perhaps this would not matter so much if the "evidence on oath" directed the Solicitor General's attention to one of the three tests. However, the so-called 'applications' which are the "evidence on oath" have usually *not* indicated within which category the Director General has considered the circumstances to fall.

98. Section 16(2) of the Official Secrets Act should be compared with section 178.13(1) of the Criminal Code which requires a judge to be satisfied

(a) that it would be in the best interests of the administration of justice to do so (i.e. to give the authorization); and

(b) that other investigative procedures have been tried and have failed, other investigative procedures are unlikely to succeed or the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures.

While we acknowledge that part (a) of this test is not appropriate for national security intercepts, we think that it is just as important in the national security context as in the criminal investigation context that consideration be given to the factors set out in (b) in justifying the authorization of what otherwise would be an unlawful invasion of privacy by electronic means for those factors relate to necessity. We shall recommend that the statute governing electronic surveillance for national security purposes be amended to provide expressly the same criteria as those required to be satisfied under section 178.13(1)(b) of the Criminal Code and additional criteria that are pertinent to the collection of security intelligence. This should not be interpreted as requiring the security intelligence agency to exhaust other investigative measures before it can obtain a warrant. The section in the Code does not require that as a condition; it is only one of three alternative prerequisites. To require as a condition that other investigative measures have been exhausted would be unduly restrictive, for, as

in the case of criminal investigations, there undoubtedly will be circumstances in which no other investigative measures have even been attempted, and from the very circumstances of the case it would be impractical to carry out the investigation of the matter using other investigative procedures only; or the matter may be specially urgent.

99. In addition to incorporating the tests contained in section 178.13(1)(b), a clearer and more appropriate test should be adopted for assessing the national security purposes to be served by electronic surveillance. The confusing tripartite test now contained in section 16(2) of the Official Secrets Act should be replaced by language requiring that the person issuing the warrant be satisfied by evidence on oath that the use of an electronic surveillance technique is necessary for obtaining information about any one or more of the following activities:

> (a) activities directed to or in support of the commission of acts of espionage or sabotage (espionage and sabotage to be given the meaning of the offences defined in sections 46(2)(b) and 52 of the Criminal Code and section 3 of the Official Secrets Act);
>
> (b) foreign interference, meaning clandestine or deceptive action taken by or on behalf of a foreign power in Canada to promote the interests of a foreign power;
>
> (c) political violence and terrorism, meaning activities in Canada directed towards or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political objective in Canada or in a foreign country.

The warrant should indicate the type of activity of which the targetted individual or premises is suspected. In the previous chapter we have set out our reasons for preferring the wording set out in (a), (b) and (c) above to that which is now used in the definition of subversive activities in section 16(3) of the Official Secrets Act. Briefly it should be recalled that this language, among other things, makes it clear that electronic surveillance might be used to collect information about terrorist groups whose activities are directed against foreign countries and eliminates the dangerously broad and ambiguous phrase

> (c) activities directed toward accomplishing governmental change within Canada or elsewhere by force or violence or any criminal means.

Indeed, as we explained in the previous chapter we believe that intrusive investigative techniques such as electronic surveillance should not be used when there is no reason to believe that the activity of an individual or group goes beyond the expression of revolutionary subversive ideas.

100. With the adoption of clearer and more precise statutory tests for using electronic surveillance to obtain information about threats to national security, we think it would be appropriate for a judge rather than a Minister to issue warrants for national security intercepts. Earlier in this chapter, we presented our principal reason for requiring a judge rather than a Minister to make the authoritative determination of whether the facts of a particular case satisfy the statutory standard for the use of certain extraordinary investigative techniques. But here let us consider what might be the most formidable objections to our

recommendation to have a judge rather than a Minister issue warrants authorizing electronic surveillance.

101. First, it might be argued that the question of whether an individual or group constitutes a sufficient threat to national security to justify an electronic intrusion should be decided by Ministers who, unlike judges, are accountable to Parliament and ultimately to the electorate for national security policies. We agree with part of this argument. Ministers are responsible for the national security activities of government; in particular, the Solicitor General, as the Minister responsible for the security intelligence agency, is responsible for the investigative policies and practices of that agency. That is why we think the Solicitor General should approve proposals by the agency to use electronic surveillance (and other intrusive techniques). He should approve such proposals from a policy point of view. But he and the Cabinet must discharge their responsibility for national security policy within the law. When the law establishes a carefully defined standard for exercising an investigative power which would otherwise be a criminal offence, there is, in our view, no derogation of ministerial responsibility in denying Ministers the final authority to determine whether a particular case meets that standard. Our system of government is not based on the single principle of ministerial responsibility: it involves other important principles, one of which is the rule of law. In a system of responsible Cabinet government operating within the rule of law Ministers are responsible for the effective and proper execution of the powers lawfully available to government, but they do not have the final responsibility for determining what the law is. In our system of government this is normally the function of judges.

102. We should emphasize that we are not suggesting that the Minister should be indifferent as to whether a proposal to employ electronic surveillance meets the legal requirements. On the contrary, he and his advisers should thoroughly scrutinize proposals from a legal as well as a policy point of view before approving an application for a judicial warrant. But our review of the administration of section 16 of the Official Secrets Act has indicated to us that there is not sufficient assurance that in every case Ministers will carefully and judiciously apply their minds to all of the legal requirements for the use of this extraordinary power. We think that judges are more apt to have the appropriate experience and to be operating in an appropriate setting for making that kind of determination of the law. As we argued earlier, normally the courts determine the legality of government action only when it is challenged after the fact. However, because the effective use of this power should always be secret, no such *ex post facto* challenge is possible by persons who may be subject to an unlawful exercise of the power. Therefore, we think it necessary that a judicial determination of lawfulness be made before the power is exercised.

103. A second possible objection to our proposal is that it is too cumbersome and imposes too many procedural requirements on the conduct of national security investigations. Granted, the proposal would add one extra step to the decision-making procedure; we do not think this constitutes a serious handicap. Since the aim of most national security investigations is to collect information well in advance of an actual act of espionage, foreign interference or terrorism,

an extra few hours should not, in most circumstances, mean that it becomes too late to obtain important information. To provide for the exceptional occasion, when even such a slight delay would jeopardize an important national security investigation, there should be an emergency clause allowing the Minister to authorize an electronic intrusion without a judicial warrant for a maximum of 48 hours. The use of this power in emergency circumstances should be reviewed by the independent review body we are proposing (the Advisory Council on Security and Intelligence) and that body should report to the Parliamentary Committee on Security and Intelligence any situations in which it believed that the emergency use had not been justified.

104. To ensure the availability of reasonably experienced judges to hear applications for warrants, we propose that five judges from the Trial Division of the Federal Court of Canada be designated by the Chief Justice of the Federal Court to hear applications. If it were considered desirable to have judges available outside Ottawa for this purpose, there are members of provincial superior courts who, at the request of the Chief Justice of the Federal Court and with the approval of the Governor in Council pursuant to section 10(1) of the Federal Court Act, act as judges of the Federal Court. They are resident across Canada and some of them might be designated to review emergency applications. However, this may not be necessary, as the warrants issued under section 16 have, so far as we know, always been applied for and granted in Ottawa, with the exception of the occasional case when the Director General has had to go to the Minister when the latter was outside Ottawa. We think that the refusal of a judge to grant a warrant should be appealable to three judges of the Federal Court of Appeal. This would ensure the government some recourse in the event that a judge of first instance adopted what appeared to be a particularly idiosyncratic view of the law. To prevent 'judge shopping', an applicant should be required to disclose to the judge the details of any application made previously with respect to the same matter.

105. We believe that the choice of the best procedure should be based on an appreciation of Canada's security needs and the working of Canadian institutions of government. Nevertheless, it is relevant to ask those who believe that Canada's national security will not be adequately protected, if Federal Court judges rather than Ministers grant warrants for electronic intrusions, to examine the experience of the United States. There, although the United States Constitution assigns the President power over foreign affairs, since 1978 the use of electronic surveillance within the United States for foreign intelligence purposes has been governed by an Act of Congress which, whenever the communications of United States persons are involved, requires an order approved by a Federal Court judge based on an application approved by the Attorney General of the United States.[18] We are not aware of any submissions by the executive branch in the United States to the effect that the requirement

[18] *Electronic Surveillance Within the United States for Foreign Intelligence Purposes*, Public Law 95-511, 95th Congress, October 25, 1978.

of judicial warrants for national security intercepts has significantly weakened the investigative capacities of that country's intelligence agencies.

106. The procedure we propose might also be objected to on the ground that it does not go far enough to ensure the proper application of the law governing electronic surveillance for national security purposes. Hearings before a judge in our proposed system would be *ex parte* proceedings. As is now the case with applications for warrants under section 178.15 of the Criminal Code and under section 443 governing search warrants, no one would be present to argue against the application for the warrant. Submissions have been made to us that the proceedings should be made more adversarial by providing for the appointment of an officer to serve as 'a friend of the court'. This officer would appear before the judge and point out possible weaknesses or inadequacies in applications. While we think such a proposal has considerable merit and have considered it carefully, we have concluded that, on balance, it would not be advisable to adopt such a mechanism. The adversarial element afforded by such a procedure might be rather artificial and would make the process of approving applications unduly complex. Further, we think that an experienced judge is capable of giving adequate consideration to all relevant aspects of an application without the assistance of an adversarial procedure. Finally, the continuing and systematic review of the use of extraordinary powers by our proposed independent review body (the Advisory Council on Security and Intelligence) should provide an adequate means of ensuring that the system of control is working as was intended by Parliament.

Renewals of warrants

107. In Part III, Chapter 3, we pointed out that, in contrast to section 178.13(3) of the Criminal Code, section 16 of the Official Secrets Act makes no provision for the renewal of warrants. We also noted that, despite the absence of legal authorization for renewals, Solicitors General at the end of each year approved the renewal of large batches of warrants. This deficiency in the law governing electronic intrusions for national security purposes should be remedied. The law should not only require, as it now does, that the warrant specify the length of time for which it is in force, but it should also establish a maximum time period for warrants and require that an application for a renewal be treated as if it were a new application. We would suggest a maximum period of 180 days. While this would be approximately 60 days shorter than the average length for warrants in the last four years for which reported statistics are available, still it is three times the maximum period available under section 178.13 of the Criminal Code for electronic surveillance for criminal investigation purposes. The statute should require not only that an application for renewal should satisfy the same criteria as apply to an application for a warrant, but, in addition, that a report be made to the judge under oath as to the nature and value of the information obtained under the original warrant.

108. In the past there has not been a sufficiently thorough review of the 'product' of the interception of communications. Some interceptions have become virtually permanent. It is true that the vast majority of warrants which

are renewed and thus last for more than a short period of time are in respect of the communications of persons or establishments suspected of undertaking foreign intelligence activities, whether those persons are foreigners or Canadians. Even in these cases, in our view, there ought to have been a more critical review of the value derived from warrants for the interception of communications. From the point of view of the Solicitor General, in our opinion it is important that such a review take place in order that he can judge, with the kind of information which should be in his possession to enable him to reach a sound judgment, the extent to which interception is "necessary" for any of the purposes set forth in the statute.

Conditions governing the execution of warrants

109. Another inadequacy of the law governing the use of electronic surveillance for national security purposes which was thoroughly examined by us and reported on in Part III of this Report concerns the means which may be lawfully used to examine, to install, to maintain and to remove an electronic interception device. As we reported in Part III, Parliament, when it enacted the Privacy Act, did not explicitly provide for the surreptitious entries which are often essential for the effective use of certain kinds of listening devices and it is at least questionable whether section 26(2) of the Interpretation Act or section 25(1) of the Criminal Code provide a basis in law for the surreptitious entry of private premises or the removal of private property for the purpose of examining, installing, maintaining or removing devices the use of which might be authorized under section 16 of the Official Secrets Act. There is also doubt as to whether there is legal authority for using the electrical power available in the premises for the operation of a device. We think these doubts should be removed. Hidden listening devices cannot, in many instances, be used effectively without the surreptitious entry of premises or removal of private property. Also they cannot be used effectively without the use of electrical power belonging to or charged to the subject of investigation or another person. The statute should expressly provide that a warrant for the interception of private communications may permit the persons carrying out the interception to enter premises or remove property for the purpose of examining the premises or property prior to installing a device or for the purpose of installing, maintaining or removing a device. The statute should also provide for the use of the domestic electrical power supply. These powers should be available only on condition that their exercise shall not cause any significant damage to premises that remains unrepaired, nor involve the use of physical force or the threat of such force against any person. The statute should require the judge who issues the warrant to specify on the warrant the powers which may be used to execute it.

110. A further problem arises relating to the installation of electronic eavesdropping devices: the possible violation of provincial and municipal regulations governing such matters as electrical installations, fire protection and construction standards. As we suggested in our analysis of these problems in Part III, Chapter 3, we think that the co-operation of the provinces should be sought to make lawful what would otherwise be unlawful under the regulations in these areas.

111. A further condition which should attach to the execution of a warrant to intercept communications for security purposes is that in every case the persons carrying out the procedure should be accompanied by a peace officer. This recommendation is particularly important when our proposal to organize the security intelligence agency as a body separate from the R.C.M.P. is adopted. Under that proposal the members of the security intelligence agency would not be peace officers. In executing a warrant which may result in a breach of the peace by a person coming on the scene, we think it important that a policeman with peace officer powers be present. Moreover, as we shall explain more fully in subsequent chapters, the requirement that security intelligence officers obtain the assistance of a peace officer in executing warrants for extraordinary powers of investigation would add a valuable countervailing power in our security arrangements.

112. The statute should not require, as it does now, that a warrant "specify the person or persons who may make the interception or seizure". That is an unnecessarily exacting requirement and one which, as we indicated in Part III, is probably not being satisfied by existing procedures. We think it would be more satisfactory for the statute to provide that a warrant be issued to "the Director General of the security intelligence agency or to any persons who act upon his directions or with his authority". If the Director General proposes to use a person who is not a member of the agency or a peace officer, he should obtain the prior approval of the Minister to the use of such person.

The scope of warrants for intercepting communications

113. Considerable doubt and confusion have existed about the types of communication which may be intercepted and the range of investigatory activity which may be authorized pursuant to warrants issued under section 16 of the Official Secrets Act. Since 1976 warrants have been issued authorizing the interception and seizure of written communications outside the course of post. This was done after an opinion had been obtained from the Department of Justice in 1976 to the effect that written communications could be intercepted under section 16 other than letters in the course of post. Members of the Security Service have also on occasion, when on premises pursuant to a section 16 warrant, used the opportunity to rummage about and search the premises beyond what was necessary for the installation of a listening device. In Part III we reviewed all of these activities and the opinions on which they were based and reached the conclusion that section 16 of the Official Secrets Act likely did not authorize the interception or seizure of any kind of written communication including mail or the search of premises. We contended that if the Security Service needs the power to enter premises to examine written documents and remove them for copying, or to intercept mail or to search premises in circumstances for which a warrant cannot be obtained under the Criminal Code or under section 11 of the Official Secrets Act, then a case must be made to Parliament and legislation passed expressly authorizing such activities. These activities must not be carried out on the foundation of an interpretation of existing law that is not free from doubt.

114. Section 16 has also been used to authorize the acquisition from telephone and telegraph companies of copies of telegrams and telex communications. Also, section 7 of the Official Secrets Act provides for a special procedure under which authorization may be given by the Minister of Justice for the acquisition from any person who owns or controls "any telegraphic cable or wire, or apparatus for wireless telegraphy" of copies of telegrams and cables. This section provides that the Minister of Justice may grant a warrant in any case where it appears "that such a course is expedient in the public interest". Until early 1971, section 7 was relied on by the Security Service to gain access to telegrams, cables and telexes. "Telegraphic warrants" were issued under this section by Ministers of Justice from 1953 onward and served upon the telecommunications companies. The outstanding telegraphic warrants, like the telephonic warrants issued under section 11, were reviewed monthly by the Minister of Justice. It is not clear how long that procedure was followed. It is known that in 1971 the Solicitor General, Mr. Goyer, began to follow a new procedure. Telegraphic communications thenceforth were assimilated procedurally with telephonic communications. Instead of applying to the Minister of Justice for a warrant under section 7, the R.C.M.P. applied to the Solicitor General for his authorization, and, if it was granted, a senior officer of the R.C.M.P., in his capacity as a Justice of the Peace, would, pursuant to section 11, issue a warrant to search and seize directed to the telecommunications company. After July 1, 1974, when section 16 came into effect, that section was relied on for the warrants issued by the Solicitor General to acquire copies of telegrams and telexes. It is quite clear that the broad terms of section 7 which allow for warrants in any case where "such a course is expedient in the public interest" are inconsistent with the specific approach spelled out in section 16 and with the philosophy of this Report.

115. In subsequent sections of this chapter we shall recommend that legislation be enacted authorizing the security intelligence agency, under an appropriate system of controls, to search premises and photograph or make copies of documents and to open articles of mail in the course of post. These powers must be expressly provided for in legislation and, under our recommendation, would require warrants separate from a warrant for the interception or seizure of communications other than a message in the course of post. Legislation authorizing the issuance of the latter warrants for national security purposes should make it clear that communication means any oral or written communication other than a message in the course of post. There are written communications such as opened letters no longer in the course of post, and telex messages, the interception or seizure of which may be as important for national security purposes as is the interception of oral communications. But the statute governing these warrants should require, as does section 16(4) of the Official Secrets Act, that a warrant specify the type of communications to be intercepted or seized.

116. As recommended in the preceding paragraphs, there should be a single statutory provision like section 16 to be relied upon as authority for obtaining the contents of telephonic communications, non-telephonic conversations, and messages passed by mail, telegram, cable or telex whether acquired by

electronic means or by acquiring copies of the printed message. Therefore, the statute should contain a clear definition of "interception" so as to cover all these situations. We suggest that this definition read as follows:

> "interception" includes listening to, recording or acquiring any communication, any written communication other than a message in the course of post, and any telecommunication, and acquiring the substance, meaning or purport thereof.

The communication of intercepted information

117. A further deficiency in section 16 of the Official Secrets Act which we discussed in Part III is that there is no protection in law for a member of the Security Service who communicates information obtained through an authorized interception to other members of the Security Service, to other departments of the federal government or to provincial, municipal or foreign governments for security intelligence purposes. We think that protection should be afforded to members of the security intelligence agency who communicate information obtained from authorized interceptions, providing such communication is for the purposes of the security intelligence agency and is in accordance with reporting rules approved by the Minister.

Reporting to Parliament

118. Section 16(5) of the Official Secrets Act requires an annual report to Parliament on the use of warrants issued pursuant to section 16. The subsection reads as follows:

> (5) The Solicitor General of Canada shall, as soon as possible after the end of each year, prepare a report relating to warrants issued pursuant to subsection (2) and to interceptions and seizures made thereunder in the immediately preceding year setting forth
>
> (a) the number of warrants issued pursuant to subsection (2),
>
> (b) the average length of time for which warrants were in force,
>
> (c) a general description of the methods of interception or seizure utilized under the warrants, and
>
> (d) a general assessment of the importance of warrants issued pursuant to subsection (2) for the prevention or detection of subversive activity directed against Canada or detrimental to the security of Canada and for the purpose of gathering foreign intelligence information essential to the security of Canada,
>
> and a copy of each such report shall be laid before Parliament forthwith upon completion thereof or, if Parliament is not then sitting, on any of the first fifteen days next thereafter that Parliament is sitting.

A report formally satisfying the requirements of subsection (5) has been filed for the years 1974 to 1978 inclusive.[19] All of the statistical information reported for these five years in accordance with the requirements of (5)(a) and (5)(b) is contained in the table below.

---

[19] A report for 1979 was filed in 1980, after the preparation of this part of our Report.

Statistics reported on use of warrants under section 16 of the Official Secrets Act, 1974-78

	1974*	1975	1976	1977	1978
Number of warrants issued	339	465	517	471	392
Average length of time in force (in days)	143	239.7	240.88	244.5	244.7

*6-month period only

119. The descriptive information required under subsection (c) and (d) has also been included in the annual reports to Parliament but in a very brief and standardized form. The "general description" of the methods of interception or seizure in the first two reports consisted of a reference to the fact that "wire tapping and eavesdropping by microphone" were used. The reports for 1976 added the information that the Solicitor General had issued a warrant authorizing the interception of postal communications but that "it could not be executed due to the prohibitive effect of section 43 of the Post Office Act". The reports for 1977 and 1978 indicated that in addition to wire tapping and eavesdropping by microphone warrants were issued for the "interception of written communication outside the course of Post". As for the "general assessment of the importance of warrants", each of the reports has contained virtually the same 'boiler-plate' language, as follows:

> (d) Warrants issued pursuant to section 16(2) O.S.A. have continued to prove of value in the detection and prevention of subversive activity both in the sphere of foreign intelligence activities directed towards gathering intelligence information relating to Canada and in the violent, terrorist or criminal activities directed towards accomplishing governmental change in Canada or elsewhere.
>
> Interceptions authorized by warrants issued pursuant to section 16(2) O.S.A. also proved indispensable investigative aids to supplement, verify or disprove information derived from other sources.

120. The bare minimum of information provided in these annual reports has not afforded Parliament an adequate basis for reviewing the operation of section 16 of the Official Secrets Act. The statistical information is apt to be misleading. For example, in giving the annual number of warrants issued, there was no disclosure that a number were merely renewals of warrants previously issued. Nor was there any disclosure that a number of the warrants issued in later years were renewals of warrants originally issued as early as 1974; that is, there was no way in which Parliament could realize that some warrants are, for all practical purposes, perpetual. The disclosure of "the average length of time for which warrants were in force" is misleading because, if the warrants that are virtually "perpetual" are treated separately, the "average length of time" for which other warrants were in force would be revealed as being significantly lower than the figure given. Above all, we regard as unhelpful the "boiler-plate" treatment of the requirement that the annual report provide "for the general assessment of the importance of warrants issued".

121. We recognize that there is a distinct problem of security in disclosing information about the use of electronic surveillance and other secretive investigative techniques which may be employed for national security purposes. That problem arises from the fact that hostile foreign intelligence agencies analyze for their own purposes every bit of information they can obtain about Canada's counter-intelligence activities. Information indicating a change in the deployment of our resources devoted to detecting foreign espionage and foreign intelligence activities may be of considerable use to such agencies. The report of the Birkett Committee in 1957 on the exercise of the power to intercept communications in Great Britain included statistics on interception for each year from 1937 to 1956. However, the Committee concluded that it would be wrong to disclose figures at regular or even irregular intervals on the grounds that

> It would greatly aid the operation of agencies hostile to the state if they were able to estimate even approximately the extent of the interceptions of communications for security purposes.[20]

Nevertheless, the very recent British White Paper on the Interception of Communications, in response to expressions of public concern about the extent of wiretapping and mail opening, has as "an exceptional measure" updated the Birkett Committee's figures. It reports the number of warrants issued by the Home Secretary for telephone wire taps and letter openings for each year since 1958. These warrants, it should be noted, may be issued in response to requests from the police and Customs and Excise officials, as well as from the Security Service.

122. We think that Parliament should have a sounder basis on which to review the exercise of the extraordinary power of investigation it has granted to the security intelligence agency. Annual statistics should be reported publicly on the number of warrants issued for each type of warrant which is available for national security investigation. (In addition to warrants for telephone wiretaps and eavesdropping by microphones, we shall be recommending warrants for concealed optional devices and cameras, or dial digit recorders, for surreptitious entries, for mail opening and for access to certain kinds of personal information held by government departments and agencies.) These statistics should clearly distinguish new warrants from warrants that are, in effect, renewals and indicate the frequency of renewals. With a statutory limit of six months on the period for which a warrant is available, we cannot see that any real purpose is served by requiring a disclosure of the average length of time of warrants. The statistical information which we propose should be annually reported may possibly be of assistance to hostile agencies. However, we think that this is a lesser evil than denying Parliament and the public an opportunity at least to monitor quantitative changes in the security agency's use of extraordinary investigative powers. The regular disclosure of accurate statistics is to be preferred to the irregular disclosure of information in response to public concern stirred up by public disclosures.

---

[20] Cmnd. 283, paragraph 152.

123. Turning to the qualitative assessment of the usefulness of the various warrants issued, we think that parliamentary review of this kind would be more effectively achieved through *in camera* meetings of a parliamentary committee than by 'boiler-plate' clauses in a public report. A full examination of the use of extraordinary powers cannot take place in public without risking great damage to the country's security. The Solicitor General should report annually to the Parliamentary Committee on Security and Intelligence his assessment of the usefulness of warrants issued in the past. In this forum, it should be possible for the Solicitor General to respond more thoroughly to questions arising from his report. Further, the independent review body (the Advisory Council on Security and Intelligence) which we shall propose, would have as one of its functions the monitoring of the entire system of special warrants for extraordinary investigative techniques. The Council's report to the Parliamentary Committee should assist members of the Committee in understanding how warrants are being used and how thoroughly the use of warrants is being reviewed by the security agency and the Solicitor General. The Parliamentary Committee should also be informed of difficulties encountered in interpreting or applying any of the statutory clauses governing the use of warrants. It should be possible to disclose much of the Committee's discussion of problems of this kind. Perhaps the wide discussion of the practice and procedure and substance of decisions made under section 16, found in this Report, and the extent to which the Government of Canada finds it possible to publish our discussion and lay it before Parliament, will provide an indication to the security intelligence agency and the responsible Minister in the future, as to what assessment and information might be laid before Parliament without imperilling the efficacy of the investigative technique or the work of the security intelligence agency generally.

Intrusions of privacy by optical devices

124. Long-distance viewing devices and miniature cameras are now available through which investigators can obtain photographs or video recordings of activities which occur or things which are located in places where there is an expectation of privacy. Future technological developments are likely to improve these devices and make them even more potent investigatory techniques. Although Parliament has not yet made it a criminal offence to oversee private communication or activity by these devices, still we believe that because they have as much potential for invading privacy as aural eavesdropping techniques, they too should be brought under an appropriate system of controls. We think that the use of hidden cameras by the security intelligence agency to film activities in places not open to the public should be lawful only under warrants issued by a judge under the same conditions as we recommended should apply to warrants for wiretapping and eavesdropping by microphone. This requirement, it should be noted, should not apply to cameras which are used in *public* places to assist in physical surveillance operations. We have not examined the use of intrusive viewing devices outside of the security context. However, this is a subject which may soon require the same legislative attention as the use of intrusive listening devices received a few years ago.

Intrusions of privacy by "pen registers"

125. An investigative device that is of occasional importance in intelligence collection is called a "pen register" by police forces. Its correct name is a "dial digit recorder". It is a small unit which is attached to a telephone company subscriber's line, usually by the telephone company. It may be used by the company to detect long distance toll frauds. It may be used by police forces and intelligence agencies to record the numbers dialled by a suspect, both local and long distance, in the expectation that this record will reveal who the suspect is dealing with. The device records the electronic impulses emitted by the subscriber's telephone when an outgoing call is made. Perforations on a tape attached to the device record the telephone number dialled, the date and time the call was made, and the duration of the call. Normally, the device does not record whether the receiving telephone was answered or the fact or substance of any conversation.

126. Legal opinions have been expressed by the Department of Justice and by one provincial attorney general that the use of pen registers does not constitute an "interception" of a "private communication" within the meaning of section 178.1 of the Criminal Code. We agree with that view. Likewise, we think that the use of pen registers need not be authorized by a Solicitor General's warrant under section 16 of the Official Secrets Act; nor need it be, for such use would not be an offence under section 178.11.

127. However, this leaves the policy question open. We think that a telephone subscriber has the same reasonable expectation of privacy in respect to the telephone calls he places as in respect to the communications he makes by telephone. The list of numbers called by a person may, just as much as a telephone conversation, reveal the most intimate details of a person's life. Knowledge that a list of numbers dialled from a telephone can be compiled by the police or a security intelligence agency without statutory authorization will inhibit the use of telephone facilities by some persons, such as journalists, in the legitimate exercise of their profession. If judicial support for the confidentiality of such information is needed, it may be found in *Glover* v. *Glover*.[21] Consequently, as in the case of the use of intrusive optical devices, even if there is no law making disclosure by the telephone company or the use of a pen register by anyone an offence, we think that the use of such devices by the security intelligence agency should be lawful only when there is a warrant issued by a judge and under the same conditions as we recommended should apply to warrants for wiretapping and eavesdropping by microphone.

WE RECOMMEND THAT there continue to be a power to intercept communications for national security purposes but that the system of administering the power and the statute authorizing the exercise of the power be changed as follows:

[21] (1980) DTC 6262 (Ont. C.A.). The case itself was concerned not with authorizing the use of a pen register but with whether the court in a child custody issue had the power to order the telephone company to disclose such information.

(1) All of the information on which an application for a warrant is based must be sworn by the Director General of the security intelligence agency or persons designated by him.

(2) Proposals for warrants should be thoroughly examined by a senior official of the Department of the Solicitor General and by the security intelligence agency's senior legal adviser, and the advice of the Deputy Minister should be available to the Solicitor General in considering the merits of proposals from both a policy and legal point of view.

(3) The legislation authorizing warrants should be amended so that, except in emergency situations, warrants are issued by designated judges of the Trial Division of the Federal Court of Canada on an application by the Director General of the security intelligence agency approved in writing by the Solicitor General of Canada.

(4) The legislation should authorize the judge to issue a warrant if he is satisfied by evidence on oath that the interception is necessary for obtaining information about any of the following activities:

(a) activities directed to or in support of the commission of acts of espionage or sabotage (espionage and sabotage to be given the meaning of the offences defined in sections 46(2)(b) and 52 of the Criminal Code and section 3 of the Official Secrets Act);

(b) foreign interference, meaning clandestine or deceptive action taken by or on behalf of a foreign power in Canada to promote the interests of a foreign power;

(c) political violence and terrorism, meaning activities in Canada directed towards or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political objective in Canada or in a foreign country;

and the warrant should indicate the type of activity of which the targetted individual or premises is suspected.

(5) The legislation should direct the judge to take the following factors into consideration in deciding whether the interception is necessary

(a) whether other investigative procedures not requiring a judicial warrant have been tried and have failed;

(b) whether other investigative procedures are unlikely to succeed;

(c) whether the urgency of the matter is such that it would be impractical to carry out the investigation of the matter using only other investigative procedures;

(d) whether, without the use of the procedure it is likely that intelligence of importance in regard to such activity will remain unavailable;

(e) whether the degree of intrusion into privacy of those affected by the procedure is justified by the value of the intelligence product sought.

(6) The legislation should provide that the Director General may appeal a refusal of a judge to issue a warrant to the Federal Court of Appeal.

(7) The legislation should provide that an applicant must disclose to the judge the details of any application made previously with respect to the same matter.

(8) The legislation should authorize the Chief Justice of the Federal Court of Canada to designate five members of the Trial Division of that court to be eligible to issue warrants under the legislation.

(9) The legislation should provide that in emergency circumstances where the time required to bring an application before a judge would likely result in the loss of information important for the protection of the security of Canada, the Solicitor General of Canada may issue a warrant which can be used for 48 hours subject to the same conditions which apply to judicial warrants. The issuance of emergency warrants must be reported to and reviewed by the Advisory Council on Security and Intelligence.

(10) The legislation should require that warrants specify the length of time for which they are issued and that no warrants should be issued for more than 180 days.

(11) Before deciding to make application to renew a warrant the Director General of the security intelligence agency and the Solicitor General should carefully assess the value of the intelligence product resulting from the earlier warrants. The legislation should stipulate that applications for renewals of warrants be treated on the same terms as applications for original warrants with the additional requirement that the judge to whom an application for renewal is made be provided with evidence under oath as to the intelligence product obtained pursuant to the earlier warrant(s).

(12) The legislation should authorize persons executing warrants to take such steps as are reasonably necessary to enter premises or to remove property for the purpose of examining the premises or property prior to installing a device or for the purpose of installing, maintaining or removing an interception device, providing that the judge issuing the warrant sets out in the warrant (a) the methods which may be used in executing it; (b) that there be no significant damage to the premises that remains unrepaired; and (c) that there be no physical force or the threat of such force against any person. The legislation should also provide for the use of the electrical power supply available in the premises.

(13) The Solicitor General should seek the co-operation of the provinces to make lawful what would otherwise be unlawful under provincial and municipal regulations governing such matters as electrical installations, fire protection and construction standards, in order to allow the security intelligence agency to install, operate, repair and remove electronic eavesdropping devices in a lawful manner.

(14) The legislation should provide for warrants to be issued to the Director General of the security intelligence agency or persons acting upon his direction or with his authority, but require that in every case the persons carrying out an entry of premises or removal of property in the course of executing a warrant be accompanied by a peace officer. If the Director General proposes to use a person who is not a member of the agency or a peace officer, he should obtain the prior approval of the Minister to the use of such person.

(15) The legislation should make it clear that warrants may be issued for the interception or seizure of written communications, other than a message in the course of post, as well as oral communications. Warrants for these interceptions must not be used for the examination or opening of mail or the search of premises. Section 7 of the Official Secrets Act should be

repealed. (See Part IX, Chapter 2 for recommendation as to total repeal of the Official Secrets Act.)

(16) The legislation should exempt from section 178.2(1) of the Criminal Code the communication of any information obtained from an interception executed pursuant to the legislation by members of the security intelligence agency for purposes within the mandate of the security intelligence agency or for the purpose of enabling the Advisory Council on Security and Intelligence or the Parliament Committee on Security and Intelligence to review the operation of the legislation.

(17) The legislation should require that the Solicitor General annually prepare a report to be laid before Parliament indicating the number of warrants for interception which have been issued during the year, the number of these which constitute renewals, and the frequency of renewals and that the Solicitor General prepare a report for the parliamentary Committee on Security and Intelligence assessing the value of the intelligence products obtained from the warrants and problems encountered in executing warrants under the legislation.

(18) The use by the security intelligence agency of (a) hidden optical devices or cameras to view or film activities in places which are not open to the public and (b) dial digit recorders ("pen registers") should be permitted only under a system of warrants subject to the conditions of control and review as are recommended above for electronic surveillance.

(21)

F. SURREPTITIOUS ENTRY

128. We have reviewed the various situations in which the Security Service has conducted searches of private premises, vehicles or baggage to look for documents or other material that would provide information about the activity of an individual or an organization which threatens the security of Canada. We have also considered the extent to which such investigative practices are authorized in other jurisdictions and the extent to which future threats to Canada's security might require the authorization of these practices. On the basis of these deliberations, we have concluded that the law should be changed to authorize the security intelligence agency, in certain well-defined circumstances and under a thorough system of control and review, to search premises and property and to photograph and copy documents.

129. We have reached this conclusion reluctantly. As we stressed at the beginning of this part of our Report, in a liberal democratic state the intrusions of the state into the private life of its citizens should be minimized. Already numerous laws authorize agents of the state to enter and search private premises and remove materials without the consent of the occupant or the owner. No addition should be made to these laws unless it can be shown that it is necessary to do so in order to protect our society from a grave danger. It is because we think that the detection of threats to Canada's security requires a power of search not now available under law that we are prepared to recommend this particular change in the law.

130. One of the reasons for the need for special search powers consists of the activities of foreign intelligence agents. Foreign intelligence agents operate in Canada under diplomatic cover or sometimes as private individuals under false identity. Both kinds of agent are usually carefully trained to communicate in ways which will avoid detection. Situations arise in which evidence needed to corroborate suspicions that a person is acting as an undercover foreign intelligence agent takes the form of equipment used for secret communications such as code books, microdot or radio equipment or personal possessions which indicate the person's true identity. Past searches carried out by the Security Service have on occasion produced such corroborating evidence — or evidence discounting the suspicion, which may also be of importance in freeing a person from suspicion.

131. In the circumstances described above, a search warrant as provided for in section 443 of the Criminal Code would usually not be available or appropriate. That section sets out the conditions under which a justice may grant a search warrant as follows:

> 443. (1) A justice who is satisfied by information upon oath in Form 1, that there is reasonable ground to believe that there is in a building, receptacle or place
>
> (a) anything upon or in respect of which any offence against this Act has been or is suspected to have been committed,
>
> (b) anything that there is reasonable ground to believe will afford evidence with respect to the commission of an offence against this Act, or
>
> (c) anything that there is reasonable ground to believe is intended to be used for the purpose of committing any offence against the person for which a person may be arrested without warrant,
>
> may at any time issue a warrant under his hand authorizing a person named therein or a peace officer to search the building, receptacle or place for any such thing, and to seize and carry it before the justice who issued the warrant or some other justice for the same territorial division to be dealt with by him according to law.

But there may be no reason to believe that there is anything in the premises of an individual suspected of developing a network of clandestine agents to work on behalf of a foreign power, which has been used or is intended to be used to commit a Criminal Code offence or will provide evidence of such an offence. Under current law, possession of espionage equipment, such as a code book or miniature camera, is not likely to point to any specific offence, nor do possessions indicative of a false identity. (In Part IX, Chapter 2, see the summary of our First Report recommendations with respect to possession of espionage equipment.) Further, even if a search warrant could be obtained for searching the premises of such a person, the procedure of obtaining and executing such a warrant will not provide for the secrecy which is necessary in counter-intelligence investigations. The opportunity of detecting the full range of a clandestine agent's network and of the capacity and intentions of his foreign handlers may be jeopardized if the search of his premises or possessions is disclosed.

132. The other provision of existing laws which might be thought to provide a sufficient basis for counter-espionage and counter-intelligence searches is section 11 of the Official Secrets Act which provides as follows:

> 11. (1) If a justice of the peace is satisfied by information on oath that there is reasonable ground for suspecting that an offence under this Act has been or is about to be committed, he may grant a search warrant authorizing any constable named therein, to enter at any time any premises or place named in the warrant, if necessary by force, and to search the premises or place and every person found therein, and to seize any sketch, plan, model, article, note or document, or anything that is evidence of an offence under this Act having been or being about to be committed, that he may find on the premises or place or on any such person, and with regard to or in connection with which he has reasonable ground for suspecting that an offence under this Act has been or is about to be committed.

This section requires only suspicion, not belief, that an offence has been or is about to be committed and relates the search warrant directly to the espionage offences in the Official Secrets Act. However, in many investigations of persons suspected of developing a base for espionage or clandestine foreign interference there will be no grounds for suspecting a specific offence, e.g. that he has communicated information that might be, or is intended to be, directly or indirectly, useful to a foreign power. We think it is essential for the government to be informed of secret foreign intelligence activities at an early stage so that it can take action to expel diplomats or prevent undercover agents from penetrating security sensitive areas of government or industry. The security of Canada requires that much protection.

133. One further deficiency of section 11 of the Official Secrets Act should be noted. That section authorizes a justice of the peace to issue the warrant. Under section 17 of the R.C.M.P. Act, R.C.M.P. officers of the rank of Superintendent and above are *ex officio* justices of the peace having all the powers of two justices of the peace. We think it would be especially wrong for warrants authorizing such searches as section 11 provides for to be obtainable from R.C.M.P. officers if the security intelligence agency, contrary to our recommendation, remains within the R.C.M.P. But, even if our structural recommendation for a security agency separate from the R.C.M.P. is adopted, we think it inappropriate for special searches relating to espionage to be authorized by justices of the peace, whether or not they are R.C.M.P. officers. Searches of this kind should be authorized only by judges who are well-qualified to apply the terms of the statute to applications. Our recommendations below provide for such a system of authorization. On this basis, we see no point in retaining section 11 of the Official Secrets Act; the search and seizure powers in the Criminal Code should prove adequate for the enforcement by the police of the offences in the Official Secrets Act.

134. The other kind of activity which we think constitutes a sufficiently serious security threat to justify investigation through a special search power is political violence and terrorism constituting a grave threat to persons or property. Modern terrorist organizations frequently employ many of the methods used by foreign intelligence agencies. They develop clandestine communi-

cations links with foreign powers and endeavour to build up networks of support behind a safe cover. Situations have arisen in the past and are likely to arise in the future, in which it is reasonable to suspect that a person or group of persons are preparing for terrorist activity but in which there is no indication of a specific offence. For instance, when a foreign intelligence agency informs Canada's security agency of the presence in Canada of persons believed to have participated in serious terrorist acts in a foreign country, there may be no indication that such persons are planning any specific act in Canada. Because of the frightening means of destruction available to terrorists, and the tremendous damage to the democratic process which can result from terrorist threats to carry out acts of violence, we think the state should not have to wait until there is reason to believe that such threats are imminent before its security intelligence agency may be employed to search the premises or property of suspected terrorists. It is because we think that these politically motivated terrorist acts pose such a threat to the whole body politic that we are prepared to recommend legislation to make lawful certain kinds of searches by the security intelligence agency which have heretofore been unlawful. We are not however prepared to recommend a similar legislative change to render lawful 'intelligence probes' for other criminal investigation purposes.

135. Our support of this change in the law is conditional on the special power of search being subject to a system of control and review similar to that which we have recommended for electronic surveillance. That system, it will be recalled, would require that applications for such searches be first approved by the Solicitor General and then submitted to a Federal Court judge who would apply a statutory test as to the kind of activity about which information may be obtained and as to the necessity for using this particular investigative technique. Warrants would stipulate the time during which the warrant could be executed and the methods which could be used to obtain entry, and would require that the persons executing the warrant be accompanied by a peace officer. The use of the power would be subject to review by Parliament and by an independent review body in the same way that we have recommended for the review of electronic surveillance warrants.

136. The legislation authorizing searches for security intelligence investigations should make it clear that the premises which may be entered under warrants also include any vehicle, vessel or aircraft and that warrants may authorize examination of the contents of receptacles such as baggage and the temporary removal of written material for examination or for photocopying purposes.

137. It may be useful in assessing our recommendation to compare it with a similar proposal made by Australia's Royal Commission on Intelligence and Security. In the Report of that Commission, Mr. Justice Hope concluded that

> 164... ASIO (The Australian Security and Intelligence Organization) should have limited and controlled right of examination and search; the right should be exercizable only upon warrant granted by the Minister, and only where the Minister has been satisfied that there are reasonable grounds to believe that documents or records may be situated on the premises without which, or without intelligence concerning which, ASIO's

function of collecting security intelligence, in respect of an important matter under investigation, would be seriously prejudiced.

165. The right should not be exercizable in relation to domestic subversion unless the Minister is satisfied that the person or organization occupying or using the premises is already engaged in subversive activities.

166. These warrants, which should be exercizable at any time, should be limited to searching for documents and records, and should authorize their inspection, copying or removal. ASIO should be required to make a report to the Minister concerning the results of any such entry or search.[22]

This recommendation was closely followed by the Australian Parliament in enacting the Australian Security Intelligence Organization Act of 1979.[23] Section 25 of that Act provides as follows:

25. (1) Where, upon receipt by the Minister of a request by the Director General for the issue of a warrant under this section, the Minister is satisfied that there are reasonable grounds for believing that there are in any premises any records without access to which the collection of intelligence by the Organization in accordance with this Act in respect of a matter that is important in relation to security would be serious impaired, the Minister may, by warrant under his hand, authorize the Organization to do such of the following acts and things as the Minister considers appropriate in the circumstances but subject to any restrictions or conditions that are specified in the warrant, namely

(a) to enter the premises;

(b) to search the premises for the purpose of finding records relevant to that matter and, for that purpose, to open any safe, box, drawer, parcel, envelope or other container in which there is reasonable cause to believe that any such records may be found;

(c) to inspect or otherwise examine any records found in the premises and to make copies or transcripts of any record so found that appears to be relevant to the collection of intelligence by the Organization in accordance with this Act; and

(d) to remove any record so found for the purposes of its inspection or other examination, and the making of copies or transcripts, in accordance with the warrant and to retain a record so removed for such time as is reasonable for those purposes.

(2) The Minister shall not issue a warrant under this section on a ground that relates to domestic subversion unless he is satisfied that a person or organization occupying or using, or that has recently occupied or used, the premises specified in the warrant is engaged in activities constituting, or in preparation for, domestic subversion.

(3) A warrant under this section shall state whether entry under the warrant may be made at any time of the day or night or only during specified hours and may, if the Minister thinks fit, provide that entry may

---

[22] Australia, *Fourth Report of Royal Commission on Intelligence and Security*, Vol. I, 1977, p. 93.

[23] Australian Security Intelligence Organization Act, 1979, section 25.

be made, or that containers may be opened, without permission first sought or demand made and authorize measures that he is satisfied are necessary for that purpose.

(4) A warrant under this section shall specify the period for which it is to remain in force, being a period not exceeding 7 days, but may be revoked by the Minister at any time before the expiration of the period so specified.

(5) Subsection (4) shall not be construed as preventing the issue of any further warrant.

In one sense our proposal would go further than the Australian legislation, in that we would not confine such a search power to records but would extend it to espionage equipment and possessions indicating a false identity. But, in another sense, our proposal does not go as far as the Australian legislation in that we would limit the availability of this investigative technique to espionage, sabotage, foreign interference, serious political violence and terrorist activities, whereas in Australia the power could also be used in relation to domestic subversion. Under the definition section (section 5) of the ASIO Act of 1979, domestic subversion includes activities which are "likely ultimately" to involve the use of force or violence to overthrow the government and activities "directed to promoting violence or hatred between different groups of persons in the Australian community so as to endanger the peace, order and good government of the Commonwealth". Further it should be noted that our proposal would require that a different and, we believe, a more exacting test of necessity be applied in deciding whether to grant a warrant and that a judge rather than a Minister issue the warrant. Also, review by Parliament and an independent review body are not features of the Australian scheme.

WE RECOMMEND THAT the security intelligence agency be authorized by legislation to enter premises, to open receptacles and to remove property for the purposes of examining or copying any document or material when it is necessary to do so in order to obtain information about activities directed towards, or in support of, espionage or sabotage, foreign interference or political violence and terrorism, providing that this investigatory power is subject to the same system of control and review as recommended above for electronic surveillance.

(22)

WE RECOMMEND THAT section 11 of the Official Secrets Act be repealed.

(23)

G. EXAMINING MAIL

138. In Part III we reviewed the Security Service's practice of obtaining information by examining the envelopes or covers of items being sent through the mail or by opening and examining the contents of such items, and concluded that these mail check operations violated provisions of the Post Office Act. (The Security Service's code name for these operations was "Cathedral".) However, at the end of that chapter we expressed the view that the law should be amended to permit the examination of mail to or from

persons if it is reasonable to believe they are engaged in activities dangerous to the security of Canada, providing such examinations are subject to an adequate system of control. Here we wish to elaborate on our reasons for taking that position and to put forward our recommendations for legislative changes.

139. Our assessment of the intelligence product of previous limited operations was that it has been of only marginal value. The following cases have been brought to our attention. One such operation was the investigation surrounding the Japanese Red Army terrorist, Omura. Two unauthorized Cathedral 'C' operations (mail openings) were performed during the Omura investigation, one authorized Cathedral 'B' operation (photographing or otherwise scrutinizing envelope but not opening it), and an authorized telephone interception. It is clear from the evidence that the telephone intercept provided evidence of a definite interest on the part of a Toronto resident in the affairs of the Japanese Red Army. However, this technique did not provide any specific indication of a link between the Toronto resident and Omura, until almost a year after the authorization for electronic interception was granted, when the terrorist arrived in Toronto.

140. The first Cathedral 'C' operation was undertaken to determine what other telephone lines were being used by the Toronto resident which might have to be tapped. This particular avenue proved inconclusive. Cathedral 'B' operations demonstrated the first concrete link between Omura (or "Joe", as he was known) and the Toronto resident when it was noted that on April 8, 1976, the Toronto resident received a registered letter from "Joe". The Toronto resident replied to "Joe" on April 13, 1976. This correspondence, as the second unauthorized Cathedral 'C' operation disclosed, consisted of two sets of applications to the University of Toronto, and established a clear link between the Toronto resident and Omura. It also established that Omura intended to visit Toronto. It is true that the telephone intercept had already indicated on April 12 that the wife of the Toronto resident had made inquiries at the University of Toronto concerning applications by foreign students in the Department of Political Economy, but, without the mail interception, that in itself would not have been sufficient to reveal the personal application of Omura.

141. Three R.C.M.P. members who testified before us concerning the case clearly indicated that they considered the use of Cathedral operations to have been vital to the resolution of this case. One of the witnesses indicated that without the results produced by the Cathedral operations, surveillance of the Toronto resident would not have been a priority item past April or May of 1976, and that, because of the scarce technical resources available to the Service, the telephone intercept would probably have been discontinued long before the expiry date of December 31, 1976, specified in the warrant. In other words, without opening the mail the Security Service would not have known that Omura intended to come to Canada, ostensibly to study, and the Service might have decided by the middle of 1976 to terminate its telephone tapping operation.

142. Another example of the use of mail opening by the Security Service will be published by us in edited form. Two Canadians who were members of an organization that the Security Service believed to be subversive travelled to a foreign country in the fall of 1970 and there was evidence that their expenses had been paid by a Canadian who was suspected of being a foreign intelligence agent. Earlier intelligence had suggested that this person had links with several violence-oriented Quebec-based revolutionary organizations. The Security Service had information that the country to which the Canadians were travelling was training guerrillas of other countries during 1969 and 1970. The Security Service was concerned that the violent guerrilla activity in that country and in another country might be planned for Canada. Consequently the Security Service began an intensive investigation in Canada of activities directed by what was "later established" to be the intelligence service of the foreign country. During the investigation, the Security Service opened the mail of the Canadian who paid the expenses of the two Canadians and other suspected agents. According to the Security Service, this helped to establish the identities of other persons whom the agent might be approaching to become agents of the foreign country in Canada, the mailing addresses of the foreign intelligence agency's handlers who were operating in several countries, and the links that existed with "several leading...Communists" both in Canada and abroad, who were supporting the activities of the foreign agents in Canada. The mail opening was complemented by surreptitious entries and electronic surveillance which produced evidence of cryptographic systems that were used by the Canadian-based foreign agents to communicate with the handlers in other countries; this enabled deciphering of the messages opened in the mail. The surreptitious entries also uncovered accommodation addresses being used by the foreign agency in several countries; helped in determining the channels and the amounts of money being used in financing the foreign agency's operators in Canada; helped to identify the structure and the executive of the revolutionary groups in Canada that were supporting the agents, and produced evidence that the Canadian who paid the travel expenses was being directed by the foreign agency and that he himself had recruited other agents in Canada. At the conclusion of the investigation, the premises of the three principal targets of the investigation were searched under warrants issued pursuant to section 11 of the Official Secrets Act, and the people were interviewed by the Security Service. No charges were laid, but one of the three returned to the foreign country to live there, and the Security Service believes that the activities of the foreign agency in Canada "subsided markedly after this event" (Vol. 315, p. 301406).

143. We also examined summaries, prepared by the Security Service, of 67 Cathedral 'C' operations, of which 55 had been authorized by Headquarters and 12 had not been so authorized. These 67 cases may be categorized as follows:

(a) 10 cases are considered by the Security Service to have produced an "important contribution to investigation". Of these 10 cases, the Security Service did not provide details as to the result in six cases; in four cases handwriting samples that were obtained proved to be useful; and in one the results were negative and were "important" only in the sense that they

contributed to the conclusion that the subject was not the agent of a foreign power.

(b) 17 cases are considered by the Security Service to be cases in which the opening of letters produced an "investigative lead", but no details of the "investigative lead" were given to us in 14 of the cases, and in a 15th case the information produced by the opening was a list of addresses of persons in contact with a suspected foreign agent. In the 16th case a known foreign intelligence officer had a close relationship with a federal government employee and once had been observed opening the employee's mail box; it was suspected that the employee was functioning as a "live letter box" (as a contact for mail to the intelligence officer), but the Cathedral "C" operation produced nothing of investigative value according to the summary provided (and contrary to the evaluation list provided). In the 17th case considered by the Security Service to have provided an "investigative lead", the envelope mailed by a known foreign intelligence officer was found to contain an application for a subscription to a small-town Canadian newspaper.

(c) In 12 cases the Security Service considers that "no intelligence of value" was obtained: in several, "semi-clandestine" contacts between the subject and a foreign military attaché had led to suspicions that Canadian military information might be passed; in another a Canadian had met clandestinely with an "agent of influence" of a foreign country; in most of the remainder of cases the subject was a known or suspected terrorist.

(d) In 16 cases, the Security Service reported that there was no evidence that mail was received.

(e) In 6 cases, Cathedral 'C', while authorized either at Headquarters or locally, was not carried out.

(f) The remaining 6 cases, while summarized, were not the subject of any evaluation by the Security Service as to whether the operation produced any intelligence of value. We do note that in one of these cases something of value appears to have been obtained: the names of the friends, relatives and contacts of a suspected foreign intelligence agent.

144. Two other cases are in the public domain. One is that of Mr. George Victor Spencer, the Vancouver postal employee who by 1960 had been recruited by a K.G.B. officer who was a member of the staff of the embassy of the U.S.S.R. According to the Security Service, Mr. Spencer admitted in his interrogation in 1965 that the tasks assigned to him included the use of his name and address as a "live letter box". Three test letters were sent to Mr. Spencer by the Soviet handler. As a signal, a small portion of a corner of the stamp had been removed and there was a small ink dot on the flap side of the envelope. His instructions were to deliver such letters unopened to his Soviet handler, who could thus examine them to determine whether they had been tampered with in the post. In addition, the Soviet handler made arrangements for meetings by sending an apparently innocuous message by mail, containing the date of the meeting. That message was to be responded to by an apparently innocuous letter of reply, which was to indicate whether the appointed date was

acceptable to Mr. Spencer.[24] During this investigation the Security Service says that it did not examine any of Mr. Spencer's mail, but speculates that the investigation might have been expedited if his mail had been opened. In any event, the case is useful as evidence of the use of the mail in Canada in an espionage operation.

145. So is the case of Mr. Bower E. Featherstone, a federal government employee who had access to classified material. Mr. Featherstone, when interviewed in 1966, denied having passed any classified material to the Soviet Union, but admitted that he had acted as a live letter box and had passed five letters from an unknown source to a Soviet handler and received payment for his services. Featherstone was charged and convicted under the Official Secrets Act because he had obtained and retained a naval chart which could have been "of assistance to a foreign power, to wit, the Soviet Union", (he had not delivered it). The use of Featherstone as a live letter box was disclosed in court by the Crown prosecutor.[25]

145A. In 1978 the officer in charge of counter-espionage reported that he had received information that a resident of Canada had requested instructions in what appeared to be an operation in an ethnic community in Canada. The R.C.M.P. Security Service suspected that instructions were given by letter, but because mail opening is illegal there was no way to find out.

146. Clearly, the case for recommending legislative authorization of mail examinations for national security purposes cannot be based solely on the value of the intelligence obtained from mail check operations in the past. These results of past operations do not settle the question of whether in the future, in order to obtain important information about threats to Canada's security, it may be necessary to examine mail, or the question of whether a law permitting the examination of mail of persons believed to be participating in acts directed towards or in support of espionage, secret foreign intelligence or terrorist activities will deter the use of Canada's postal system as a channel of communication for these activities. Our consideration of these two questions about the future brings us to recommend mail examinations for security purposes.

147. Agents of foreign intelligence services and members of terrorist groups are almost always very difficult to detect. They are usually individuals who are intelligent, dedicated to their cause, and well-trained in the art of avoiding detection by police or security officers. It is in their communication links that such persons are often the most vulnerable. We think it is unwise to guarantee them a free and convenient channel of communications within Canada by exempting all mail communications from lawful examination by security officers. Therefore, we believe it prudent that, in cases where there are reasonable grounds to believe that the mail is being used by persons for the

[24] Most of the foregoing was described in the *Report of the Commission of Inquiry into Complaints made by George Victor Spencer*, July 1966. The Commissioner was the Honourable Mr. Justice D.C. Wells.

[25] April 4, 1967. The prosecutor was Mr. P.T. Galligan, who disclosed this aspect of the case when speaking to the accused's sentence. The transcript does not reveal that the source of the information was Mr. Featherstone himself. See the *Ottawa Citizen*, April 5, 1967.

purpose of working secretly on behalf of a foreign power in Canada or of advancing the cause of a terrorist organization, the security intelligence agency should have access to any item in the course of mail as a means of furthering its investigation.

148. Against these considerations must be weighed the intrusion of privacy which will result. The mail is virtually the only means of communication left in our Canadian society into which the state cannot intrude without the individual's consent. A decision to weaken this one remaining citadel of private communication requires a very careful balancing of the respective weights which should be given to these competing concerns of national security and individual privacy. It is important to bear in mind that we are not dealing with absolutes. We doubt that the staunchest proponent of thoroughness in the protection of national security could demonstrate that Canada's security — as we have defined that concept — will be absolutely imperilled if Canada's security intelligence agency is denied the power of examining mail. But, by the same token, the privacy of postal communication would not be absolutely abolished for all citizens and residents of Canada by legislation which would permit a security intelligence agency, under judicial warrant, to examine the mail of persons who it reasonably believes are participating in espionage, foreign interference or terrorist activities.

149. This last point is important in that it refers to the conditions and controls which, in our view, must attach to an acceptable mail-opening system. Indeed our support for a legislative amendment authorizing mail examinations for national security purposes is conditional on such legislation prescribing conditions and controls similar to those which we have recommended for electronic surveillance and the search of private premises or property. An important objective of our review of the operation of section 16 of the Official Secrets Act was to assess the adequacy of that law as a means of regulating the interception of communications in national security investigations. Because of the many inadequacies we found in the provisions of that section and in its administration, we think it would be a mistake to extend that section to mail without redefining the conditions under which the power may be used and strengthening the system of controlling and reviewing its use along the lines we have recommended above.

150. One change in the provisions of section 16 which is particularly important in the context of mail opening is the definition of subversive activity in relation to which communication may be intercepted. Among other things, the definition which is now contained in section 16(3) makes it possible to intercept communications of persons whose subversive activity does not go beyond expressing ideas which call for the ultimate overthrow of our system of government or organizing a demonstration or protest strike to bring about a change in government policy. The definition of "subversive or hostile activities" found in section 15(2) of the Access to Information Bill recently tabled in the House of Commons (Bill C-43), is no improvement in this respect, as it still contains the dangerously ambiguous reference to

> (d) activities directed toward accomplishing government change within Canada or foreign states by the use of or the encouragement of the use of force, violence or any criminal means.

In our view the power to examine mail for the purpose of protecting national security should be used only if it is necessary to obtain information about an individual or group who, it is reasonable to believe, is engaging in activities directed towards or in support of espionage, sabotage, clandestine or deceptive actions to promote the interests of a foreign power in Canada, or acts of serious violence against persons or property for the purpose of achieving a political objective in Canada or in a foreign country.

151. Suggestions have been made that a power which constitutes so grave an encroachment on privacy as mail opening should be used only against foreigners, and not against Canadian citizens. Quite apart from obvious practical difficulties, we cannot accept this suggestion. It is not the nationality of individuals that determines whether their activities threaten security: it is the seriousness of the threat of these activities and the need to obtain advance information about them that constitutes the rationale for intercepting private communications. In any case, we look with disfavour on an approach to civil liberties in Canada which takes the position that the liberties which non-citizens in Canada may enjoy under Canadian law should be less than those enjoyed by citizens.

152. The system of granting warrants for the examination of mail and of reviewing the use of such warrants should be essentially the same as that which we have recommended for electronic surveillance and the search of private premises or property. Warrants should be issued to the Director General by a Judge of the Federal Court on the basis of an application approved by the Solicitor General and with evidence given under oath as to the necessity of using this particular investigative technique. The statute should direct the judge to consider the same matters in determining whether there is necessity as when hearing applications for warrants to intercept communications for purposes of criminal investigation under section 178.13(1)(b) of the Criminal Code. The use of warrants and the operation of the legislation should be subject to review by Parliament and the Advisory Council on Security and Intelligence on the same basis as recommended for electronic surveillance and searches of premises or property.

153. The legislation providing for the examination of mail by the security intelligence agency should require that a warrant be obtained for the examination of all classes and types of mail and for obtaining information from the envelopes or exterior covers of items in the course of post as well as from the contents of mail. The legislation should expressly state that its provisions for the issuing of warrants shall prevail over section 43 of the Post Office Act, and the latter section should be amended to make this possible.

154. Warrants should specify the ways in which articles are to be examined. It may be sufficient to obtain information from mail covers and not necessary to read the contents. There should be authorization for copying the covers or contents of mail, and for temporarily removing the article from Canada Post premises. We think it would be impracticable to adopt the suggestion made in one submission to the Commission that warrants specify the letters to be opened. It is impossible to predict the specific letters or parcels which may

contain relevant information or material. Warrants should be issued for the interception of mail addressed to, or sent by or from, a specified person or address. The latter possibility is necessary to provide for a situation in which it is suspected that a false name is being used. Warrants should also specify the length of time during which a warrant may be used within the same maximum time period and subject to the same renewal conditions as we have recommended for electronic surveillance and searches. We note that section 27(4) of Australia's ASIO Act imposes a 90-day time limit on warrants for postal inspections as compared with a six-month limit on electronic surveillance warrants. However, we cannot see why there should be a difference in the maximum periods for which the two kinds of warrants are available. In both cases, six months should be treated as a maximum and every effort should be made to confine the length of time for which a warrant is requested and granted to the period when it is reasonable to expect significant communications to occur. Because breaches of the peace do not occur in executing a warrant to examine an article in the course of post, it would make no sense to require that a peace officer be present when these warrants are being carried out. However, the legislation should require that the Post Office Department be informed whenever a warrant is issued and when warrants expire. Further the legislation should require the co-operation of postal officials with members of the security intelligence agency in carrying out the procedures specified in a warrant.

155. In judging whether articles of mail should be inspected for national security purposes and if so, under what conditions and controls this should be done, Canadians will no doubt wish to base their decisions on an assessment of Canada's security needs and on the ideals of civil liberty which derive from Canadian traditions and aspirations. Still, in arriving at a decision and in assessing the recommendations of this Commission on this subject, it may be useful to look at the laws and policies of countries whose system of government and democratic principles are close to our own. In the United States, although the Rockefeller Commission and the Church Committee disclosed widespread improper surveillance of the mails by intelligence agencies, U.S. mail is not made immune from lawful inspection for national security purposes. The President's Executive Order of January 21, 1978[26] attempted to control national security mail checks by providing that:

> 2-205. Mail Surveillance. No agency within the Intelligence Community shall open mail or examine envelopes in United States postal channels, except in accordance with applicable statutes and regulations. No agency within the Intelligence Community shall open mail of a United States person abroad except as permitted by procedures established pursuant to section 2-201.

Generally the control system is stricter where there is no suspicion of any foreign involvement. First class mail which originates in the United States cannot be opened without a showing of "probable cause" (i.e., a belief that evidence of a crime will be discovered) unless consent has been secured or an

[26] Executive Order 12036; January 21, 1978.

emergency exists. Letters opened for foreign intelligence purposes may be an exception to this rule. Mail cover checks are permitted under Postal Service regulations which require a written request from a law enforcement agency specifying "reasonable grounds" which demonstrate that the mail cover is necessary to

(a) protect the national security,

(b) locate a fugitive, or

(c) obtain information regarding the commission or attempted commission of a crime.[27]

The "reasonable grounds" requirement is a standard which appears to be less demanding than the "probable cause" requirement of the Fourth Amendment of the U.S. Constitution. In late 1978 a Federal Court Judge declared this national security ground to be unconstitutionally vague. In August 1979, new regulations were adopted by the Postal Service defining the phrase "to protect the national security" to mean:

> to protect the United States from any of the following actual or potential threats to its security by a foreign power or its agents:
>
> (i) an attack or other grave hostile act;
>
> (ii) sabotage, or international terrorism; or,
>
> (iii) clandestine intelligence activities.[28]

In Great Britain authorization to examine mail for criminal investigation, customs or security purposes is obtained through the same process of ministerial warrants as applies to telephone interceptions. The recent White Paper on this subject discloses that over the past 20 years the highest number of warrants for mail opening issued by the Home Secretary in any one year has been 139 and the lowest, 44.[29] However, these figures do not indicate how many of these warrants were issued for national security investigations. Finally, in Australia, following the recommendations of the Royal Commission on Security and Intelligence, provision for examining mail has been included in the Australian Security Intelligence Organization Act.[30] Warrants for examining mail are issued on terms and conditions similar to those set out in section 25 (reproduced above) with respect to searches.

> **WE RECOMMEND THAT, notwithstanding the present provisions of the Post Office Act, the security intelligence agency be authorized by legislation to open and examine or copy the cover or contents of articles in the course of post when it is necessary to do so in order to obtain information about activities directed towards or in support of espionage or sabotage, foreign interference or serious political violence and terrorism, providing that this investigatory power is subject to the same system of control and review as recommended above for electronic surveillance, except that**

---

[27] 39 C.F.R. 233.2.

[28] *Ibid.*

[29] Cmnd. 7873, April 1980, Annex, Table I.

[30] Australian Security Intelligence Organization Act, 1979, section 27.

instead of requiring that a peace officer accompany persons executing warrants issued for this purpose, the legislation should require that the Post Office Department be notified when such warrants are issued and expire and that Post Office officials co-operate with members of the security intelligence organization in carrying out the procedure specified in the warrant.

(24)

H. ACCESS TO CONFIDENTIAL PERSONAL INFORMATION HELD BY GOVERNMENT

156. An important potential source of information for a security intelligence agency is personal information contained in the files and records — the so-called 'data banks' — of departments and agencies of the federal government. We say 'potential' source because under existing law the release of virtually all personal information held in federal government data banks to the R.C.M.P. is prohibited if the release is for security intelligence purposes. In the past, as we reported in Chapter 6 of Part III, the R.C.M.P. Security Service obtained confidential personal information from federal government departments notwithstanding that such practices were in some instances not authorized or provided for by law; however, in the past two or three years the legal barriers to access have been strictly observed.

157. At the conclusion of Part III, Chapter 6, we stated our view that the laws which protect the confidentiality of personal information held by the federal government should provide some means of access by the security intelligence agency to protected information, provided such access is subject to an appropriate system of control and review. Here we shall set out our reasons for recommending this change in the law and our recommendations as to the kind of legislative change which is needed.

158. Again, in considering this subject we must weigh our concern for the individual's privacy against the requirements for effectively protecting national security. Today, the enormous range of government programmes and regulation means that there are myriad circumstances in which the citizen is required to give personal information to the government in order to comply with statutory obligations or enjoy statutory benefits. Our concern about how this ever-growing volume of information which the government holds about each one of us is used, and how access to it is controlled, is not only a concern for individual privacy; part of our concern is with maintaining a relationship of trust between the citizen and government.

159. But it should also be recognized that there are important investigatory needs relating to the protection of national security which are most effectively met by affording the security intelligence agency access to certain kinds of government information. We think these needs should be served, and can be served, in a manner which will both prevent excessive disclosure of personal information and entitle the government to retain the trust of the citizen in its respect for the confidentiality of personal information.

160. The most important investigatory use of personal information in government data banks is in assisting the security agency in its efforts to identify and locate individuals. These efforts are particularly important when the subject of investigation is suspected of operating under a false cover, or when the agency is trying to discover the identity of a person reported to be in contact with a hostile foreign intelligence agency or to be associated with a terrorist organization. Information in government files is obtainable directly and expeditiously, and can often save considerable time and expense in ascertaining and corroborating identity. Information in the S.I.N. data bank, because of its universality, is one of the most useful sources of government information for this purpose.

161. Our review of cases in which the Security Service has used information in government data banks and cases in which it has requested to use such information disclosed several other important uses of this kind of information.

162. Occasionally, such requests have been made as the result of inquiries by foreign intelligence agencies. We think these requests of foreign intelligence agencies should be screened much more carefully than they have been in the past. In Chapter 7 of this part of our Report we make recommendations for strengthening the system of controlling liaison with foreign agencies and for ensuring that the security intelligence agency provides information to foreign agencies only on subjects that are within the Canadian agency's own statutory mandate. But within these limitations and controls, we think it essential that Canada's security intelligence agency be able to respond effectively to requests received from foreign intelligence agencies. The protection of Canada's security frequently requires that our own security agency obtain information from foreign agencies, including information held by departments of foreign governments about the identity of persons travelling with foreign passports in Canada. Our security agency's access to this foreign information is put in jeopardy if it cannot reciprocate by supplying information from its own government's files.

Access provided for in proposed Privacy Act

163. A legislative proposal which is currently before Parliament would remove the largest single legal barrier to a security intelligence agency's access to government information. This is the proposed Privacy Act which, along with the government's Bill on Access to Information, had its first reading in the House of Commons on July 17, 1980. This legislation could give the security intelligence agency a controlled means of access to all personal information held by government institutions except for information which is protected by other Acts of Parliament. It would accomplish this by repealing and replacing Part IV of the Canadian Human Rights Act. Section 52(2) of that Act provides as follows:

> (2) Every individual is entitled to be consulted and must consent before personal information concerning that individual that was provided by that individual to a government institution for a particular purpose is used or made available for use for any non-derivative use for an administrative purpose unless the use of that information for that non-derivative use is authorized by or pursuant to law.

When this "non-derivative use" section of Part IV became law in 1976, there was some doubt as to whether Security Service requests for information (or, for that matter, Criminal Investigation Branch requests) constituted a prohibited administrative use. However, by 1978, section 52(2) was being interpreted strictly by all departments and agencies with the result that the R.C.M.P. Security Service was now denied access to virtually all personal information possessed by other federal government institutions.

164. Section 7 of the Bill now before Parliament, which it is proposed should replace Part IV of the Canadian Human Rights Act, provides that personal information under the control of a government institution shall, subject to certain exceptions, be used only for the purpose for which it was obtained. Section 8(2) lists the exceptions, all of which are "subject to any other Act of Parliament". The exception which is most relevant for our purposes is 8(2) which would permit a government institution to disclose personal information

> (e) to an investigative body specified in the regulations, on the written request of the body, for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation, if the request specifies the purpose and describes the information to be disclosed;

Assuming that the security intelligence agency would be an investigative body specified in the regulations, it would by virtue of this clause have access to personal information in all government data banks except those to which access is barred by other Acts of Parliament. One of the important sources of security intelligence to which this legislation would restore access is information which the Department of External Affairs' Passport Office has obtained from passport applicants. However, there is some doubt as to whether the security intelligence agency under the proposed legislation would have access to S.I.N. card information. As we said in Part III, Chapter 5, it may not be open to the Minister of Employment and Immigration to release S.I.N. card information for security intelligence purposes.[31] Nor would the agency have access to income tax,[32] family allowance,[33] old age security[34] or Canada Pension Plan information[35] or census information obtained by Statistics Canada,[36] all of

[31] Section 114 of the Unemployment Insurance Act (S.C. 1970-71 Chapter 48 as amended by S.C. 1976-77, Chapter 54, Section 60.1) provides as follows:

> 114. Information, written or oral, obtained by the Commission or the Department of Employment and Immigration from any person under this Act or any regulation thereunder shall be made available only to the employees of the Commission or the said Department in the course of their employment and such other persons as the Minister deems advisable, and neither the Commission, the said Department, nor any of their employees is compellable to answer any question concerning such information, or to produce any records or other documents containing such information as evidence in any proceedings not directly concerned with the enforcement or interpretation of this Act or the regulations.

[32] Income Tax Act (R.S.C. 1970, ch.148), s.241(1).

[33] Family Allowances Act, 1973 (S.C. 1973-74, ch.44), s.17.

[34] Old Age Security Act (R.S.C. 1970, ch.O-6), s.19.

[35] Canada Pension Plan (R.S.C. 1970, ch.C-5), s.107.

[36] The Statistics Act, S.C. 1970-71, ch.15, s.16.

which are protected by Acts of Parliament which bar disclosure of information, even with the permission of the Minister, for any purpose unrelated to the programme or purpose for which the information was obtained.

165. The proposed legislation would go some way towards improving the current situation. It would give the security intelligence agency access to some of the government information it must have if it is to discharge its functions effectively. Also, it would provide a system of controlling and reviewing this access which would be a distinct improvement on the haphazard and often underhand procedures that prevailed in the past. Requests for personal information would have to be made in writing specifying the purpose for which the information was needed. Requests would be made directly to the Minister or head of the institution which holds the information. Section 8(3) requires that the Minister or head of the institution must retain a copy of the request, and, if requested by the Privacy Commissioner, provide the Privacy Commissioner with a copy of the request. The Privacy Commissioner may review, either on her own initiative or in response to an allegation by a complainant, whether personal information has been properly disclosed. While these provisions of the proposed Privacy Act represent, generally, a move in the right direction, we think they fall short of a satisfactory comprehensive solution to the issue of providing access for national security purposes to personal information held by the federal government. In certain respects, the legislation goes too far in opening up access to a security intelligence agency and in other respects it does not go far enough.

The scope of access

166. First, let us deal with what we consider to be an inadequacy in the access provided for in the proposed Privacy Act — its limitation to data banks not protected by other Acts of Parliament. We think there are circumstances in which tax information will be an extremely valuable means of identifying or detecting persons who are acting covertly on behalf of a foreign power or who are furthering the objectives of terrorist groups. For these situations the law should provide for the security intelligence agency to have access to income tax information under an appropriate system of control and review. However, while information from Family Allowance, Old Age Security and Canada Pension Plan records is not as likely to be needed for security intelligence investigations, we cannot see why the law should not provide for the same limited access to these data banks. We note that the Church Committee in the United States — which is the only other government Commission or committee in the English-speaking democracies to report on this subject — came to a similar conclusion. While it called for tight controls on the intelligence agencies' access to tax records as well as medical or social history records, its recommendations on this subject would give access to such information

> (1) In the course of a criminal investigation if necessary to the investigation;
>
> (2) If the American is the target of a full preventive intelligence investigation and the Attorney General or his designee makes a written finding that

(i) he has considered and rejected less intrusive techniques; and (ii) he believes that the covert technique requested by the Bureau is necessary to obtain information necessary to the investigation.[37]

167. One category of federal government information which it would be reasonable to exempt from the scope of legislation giving access to otherwise protected bodies of information is the census information compiled by Statistics Canada. While such information may not be more personal than that found in some other federal data banks, the tradition in this country has been very strongly in favour of complete confidentiality of census returns. The unqualified guarantee of confidentiality helps to overcome the reluctance of Canadians to respond to inquiries about personal matters for purposes which may be suspect, or at least not clearly understood, by many.

Control and review of access

168. Turning now to the system of control and review provided for in the proposed Privacy Act, we think there are a number of ways in which that system should be strengthened. The legislation does not provide a clear enough test of necessity for access to personal information for security intelligence purposes. It leaves the prior approval of all access, including access to details of a person's life far beyond what is needed for purposes of identification, to Ministers, and it provides no role in approving requests for information to the Minister responsible for the security intelligence agency.

169. In our view a satisfactory system for controlling access by a security intelligence agency to personal information in the hands of government departments must recognize a distinction between two kinds of information requiring two levels of protection. There are a number of items of what we will refer to as 'biographical information' which are extremely useful in identifying and locating individuals and which are relatively public in that such items of information about most of us are publicly available. There might be considerable room for argument as to what should be included on a list of items of such biographical information. Our own suggestion is that the list should include the following:

— full name (including change of name);

— address (including changes of address);

— phone number;

— date and place of birth;

— occupation;

— physical description.

We think that biographical information restricted to the items listed above should be accessible by a security intelligence agency through a system of administrative control similar to that provided for under section 8(2)(e) of the

[37] U.S. Senate, *Final Report of the Select Committee to Study Governmental Operations*, 1976, Book II, p. 329.

proposed Privacy Act. Under the general system for controlling security intelligence investigation that we proposed in Section B of this chapter, the security intelligence agency could make requests to government departments for this kind of biographical data in a Level Two investigation which can be initiated with no higher approval than the Headquarters of the security intelligence agency. However, access to more personal information, including information about a person's financial background, marital history, travel plans, social welfare benefits or employment history, should require a higher level of approval. Obtaining information of this kind can involve an intrusion of a person's privacy as serious as the intrusion involved in electronic surveillance, searches of premises or property, or mail-opening, and should be subject to as rigorous a system of control and review.

170. The proposed Privacy Act does not provide a satisfactory test or definition of the national security needs which may justify access to personal information in government files. Section 8(2)(e) would permit access "for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation". The first of these purposes, the enforcement of any law, is reasonably clear (although we note in passing that it establishes that an extremely minor case — for instance, the investigation of a traffic offence — may justify access to very personal information. We will examine this aspect of the legislation in Part X, where we consider legislative proposals related to the criminal investigation responsibilities of the R.C.M.P.). But the second purpose, "carrying out a lawful investigation", presumably for some purpose other than law enforcement, is not at all clear. We think it is a mistake to provide statutory authorization for security intelligence gathering in such vague terms. If statutory provision is to be made for the security intelligence agency's access to personal information in government data banks, it should be tied to a statutory definition of the purpose and scope of security intelligence investigations. Further we think that the statutory definition which is used should provide greater assurance than do existing definitions of subversive activities, including the definition contained in the proposed Privacy Act, that security intelligence investigations will not encroach on legitimate forms of political dissent. Therefore we recommend that access to personal information of both the biographical and more personal kind held by federal government departments and institutions, be accessible for security intelligence purposes only if the investigation falls within the statutory mandate of a security intelligence agency which we have recommended earlier in this Report.

171. As we have indicated, we think that requests by the security intelligence agency for personal information, beyond 'biographical information', should require a stricter method of control than that provided in the proposed legislation. Requesting additional personal information from federal government institutions of any kind should be treated as a component of a "full" investigation, the initiation of which, under the general scheme we proposed in Section B above, requires the approval of the Solicitor General. Further, personal information beyond biographical data should be accessible only through a warrant issued by a Federal Court Judge in response to an application of the Director General approved by the Solicitor General of

Canada. The issuance of the warrant should be conditional on meeting the same test of necessity we have recommended for applications for warrants for electronic surveillance, searches and mail examinations. The provision in the proposed legislation for a review by the Privacy Commissioner falls far short of an acceptable means of controlling such a potentially intrusive technique of investigation. Not only is that latter system confined to *ex post facto* review, but, under it, the Privacy Commissioner would not be informed of each instance in which access to personal information was granted. She would review only those cases where she requested a copy of the security agency's application. How is she to know when a questionable application has been made? She can also review complainants' allegations of improper disclosure: however, as we have repeatedly emphasized, it is of the essence of security intelligence investigations that the subjects of such investigations be unaware of the investigation. It is precisely for that reason that we believe a system of prior approval, involving the judicious application of a strict test of necessity, is needed as a means of ensuring that government information about the personal details of one's private life, beyond those items that are generally public knowledge, is used for national security purposes only when a clear case for the necessity of such use has been made.

172. If the scheme we recommend were to be adopted, review by the Privacy Commissioner might be retained to enable that official to carry out her general function of monitoring the protection of privacy in government institutions. But, in addition, provision should be made for the review of warrants for use in the security intelligence agency similar to that recommended for the review of other warrants authorizing the use of extraordinary investigatory powers by the security intelligence agency — i.e. Parliamentary review and review by the Advisory Council on Security and Intelligence.

173. Warrants granting access to personal information should be submitted to the Minister of the Department or head of the institution which possesses the information. The question arises whether the Minister or head of the institution should have discretion to refuse to accede to a request authorized by warrant. Situations may arise in which a Minister believes that the integrity of a programme administered by his Department is seriously jeopardized by the disclosure of personal information obtained with an expectation of confidentiality. We have considered this matter carefully and have concluded that, providing that the warrant has been granted on the basis of a showing of necessity according to the procedures we have recommended, the head of the institution receiving the warrant should not have discretion to refuse to comply with the terms of the warrant. If the Minister or head believes that a particular warrant is unreasonable, or that a series of warrants indicates excessive use of his institution's records and is unable to persuade the Solicitor General to withdraw the warrant, he could make representations to the Prime Minister and ask that the Solicitor General be directed by the Prime Minister not to execute the warrant. But if the necessity of obtaining information for the protection of national security has been determined by the Minister responsible for the security agency and according to a reasonably precise statutory standard applied by a judge, then we do not think it right to leave it to another

Minister or head of an institution to put the requirements of his Department ahead of the requirements of national security. The Prime Minister or Cabinet might decide that the integrity of some other government programme should be given more weight than protection against a particular threat to national security, but this determination of priorities should not be left to a Minister or head of an institution who has no personal responsibility for national security matters.

Personal information held by provincial governments

174. There are a number of kinds of personal information held by provincial governments or institutions under provincial jurisdiction which are useful to a security intelligence agency. In the past the R.C.M.P. Security Service has used information from the following provincial or municipal sources:

- hospital and health insurance records
- vital statistics records
- land titles records
- motor vehicle and driver's licenses
- retail tax records
- education records
- welfare records
- public utilities records
- electoral records

As we reported in Part III, information from these sources sometimes was obtained in ways not authorized or provided for by law. While we have no doubt about the security intelligence agency's need to obtain certain kinds of personal information from government institutions under provincial jurisdiction, we believe, that, with one possible exception, the legally authorized means of access which now exist are adequate and that there is no need to seek the support of the provinces for legislative amendments in this regard.

175. It is extremely important that the security intelligence agency be directed to obtain information from officials who are authorized by law to release the information and not through undercover sources. If a legally authorized means of access is not available with respect to some category of provincial information which the security agency considers essential, the matter should be raised with the Solicitor General of Canada and, if he is persuaded of the need for the information in question, he should seek the co-operation of the appropriate provincial Minister in making arrangements for a legal method of access. If the provinces adopt privacy legislation which restricts access to personal information as strictly as does Part IV of the Canadian Human Rights Act, then it may well be necessary to seek provincial support for an exception to such restrictions which would permit access by the security intelligence agency on terms similar to those we have recommended should apply at the federal level.

176. The one qualification we make to our judgment that there is no immediate need for provincial legislative change permitting security intelligence agency access to provincial government information concerns hospital and medical insurance records. As Commissioners who have had an opportunity to study national security needs, we think that we should report our findings as to the problem that existing statutory restrictions create for a security intelligence agency. Briefly, we can report that situations have arisen in the past in which information from hospital or health insurance records has been of great assistance in successfully completing investigations of persons whose activity has constituted a significant threat to the security of Canada. For example, information obtained from the details of an individual's medical history was crucial in a major counter-espionage investigation. Psychiatric information has been of importance in providing security intelligence advice to those responsible for coping with terrorist situations. We think it is likely that similar situations will arise in the future in which detailed medical information will be of great assistance in the successful completion of important security investigations. Although we have been able to examine only a sample of the legislation which governs access to medical and health records in the various provinces, we note that there are secrecy provisions in the statutes and regulations of a number of provinces which would clearly bar access by a security intelligence agency to confidential information for purposes other than the enforcement of the Hospital or Insurance Act itself. In these provinces, the statutory provisions do not permit even the Minister, Hospital Board or Insurance Commission to authorize release of medical records for security intelligence investigations.[38]

177. We think the infrequent but relatively urgent security investigation needs create the strongest case for providing some lawful means of access to medical and health information by a security intelligence agency. (As we noted earlier, we comment on this matter in more detail in Annex I where we examine the relevant recommendations of the Krever Commission.) Hospital and medical insurance records are also useful sources of biographical data in identifying and locating individuals. But we think the need for access to biographical information through hospital or medical records may be significantly reduced if the legal barriers to obtaining such information at the federal level are modified along the lines recommended above and provided for in legislation now before Parliament. Also we should note that, if the changes in the security screening procedures which we recommend in Part VII of this

[38] We examined secrecy provisions in the following Acts:

Alberta Health Care Insurance Act, Saskatchewan Medical Care Insurance Act, Ontario Health Insurance Act, Nova Scotia Hospitals Act, Nova Scotia Health Services and Insurance Act, P.E.I. Health Services Payment Act, Newfoundland Medical Care Insurance Act, Saskatchewan Hospital Standards Act, Newfoundland Medical Care Insurance Act. One statute relating to medical and health information which has no confidentiality or secrecy provisions is the British Columbia Medical Services Act (S.B.C. 1967, ch.24).

Report are adopted, there will be no need for the security intelligence agency to have access to medical information in carrying out its responsibilities in the security clearance process. If a government department considers that it needs medical information, for instance a record of a person's psychiatric treatment, in order to assess an individual's 'reliability' for a security sensitive position, under our proposals it would have to obtain that information with the individual's consent through security staffing officers in the department or from the Public Service Commission. Under our proposals, such information is not to be obtained, either openly or surreptitiously, through the security intelligence agency.

WE RECOMMEND THAT legislation authorize the heads of federal government institutions to release information concerning an individual's name, address, phone number, date and place of birth, occupation and physical description on receiving a written request from the security intelligence agency stating that such information is necessary for the purpose of locating or identifying an individual suspected of participating in one of the activities identified as a threat to the security of Canada in the statute governing the security intelligence agency, and that all other personal information held by the federal government, with the exception of census information held by Statistics Canada, be accessible to the security intelligence agency through a system of judicially granted warrants issued subject to the same terms and conditions and system of review as recommended for electronic surveillance, searches of premises and property, and the examination of mail.

(25)

WE RECOMMEND THAT warrants issued for obtaining personal information for security intelligence purposes be submitted to the Minister or head of the government institution which holds the information and that the Minister be required to comply with the warrant unless the Prime Minister directs the Solicitor General not to execute the warrant.

(26)

WE RECOMMEND THAT the security intelligence agency obtain personal information held by government institutions under the jurisdiction of provincial governments only from persons legally authorized to release such information and that, with regard to any province in which there is no authorized means of access to information to which the Solicitor General of Canada considers that the security intelligence agency should have access in order to discharge its responsibilities effectively, the Solicitor General should seek the co-operation of the province in amending its laws to make such access possible.

(27)

I. THE WARRANT SYSTEM AND PROPOSED LEGISLATION

178. We conclude this chapter by explaining how the various warrants we have recommended for the use of extraordinary investigative methods by a

security intelligence agency should be related to one another and by setting out a draft legislative basis for this warrant system.

179. Our recommendations would make the security intelligence agency's use of four extraordinary powers conditional on obtaining a warrant from a Federal Court Judge. These four powers are the interception of communications by electronic surveillance, searches of private premises or property in circumstances in which a search warrant for criminal investigation would not be available, the examination of mail, and access to personal information other than 'biographical information' held by the federal government. We refer to these powers as 'extraordinary' because they involve acts which would be violations of law if carried out by ordinary citizens, and because, unlike special police powers, they may be exercised in circumstances where there is no evidence that a particular crime has been committed or is about to be committed. Two other techniques, which are not extraordinary in this sense, namely surveillance of private premises by hidden optical devices or cameras and the use of dial digit recorders, should also be subject to this system of control by judicial warrants.

180. Under our recommendations for controlling the level of investigation, the security intelligence agency could not initiate a request for a warrant to use any of these techniques to gather intelligence about a specific individual or group until a 'full' investigation of that individual or group has been approved. It will be recalled that a decision to carry out a full investigation must be approved by the Solicitor General on a proposal which is supported by the Director General and has been carefully reviewed by a Committee which includes senior officers of the security agency as well as a lawyer from the Department of Justice and a senior official of the Solicitor General's Department. At the time the Solicitor General's approval of a full investigation is sought, the security agency might request his approval of an application to a judge for a warrant for a particular technique. It might conceivably at that time request his approval for applications for warrants for more than one technique, but in this case it would be extremely important for the security agency and the Solicitor General to give careful consideration to the necessity of using each technique. Every effort should be made to use only that method which is best calculated to enable the agency to complete an investigation with a minimum intrusion of privacy. We do not think that the various techniques requiring a judicial warrant can be scaled in terms of their inherent intrusiveness. Indeed, in some circumstances, the use of an undercover informant, which does not require a judicial warrant, may be regarded as a more intrusive and less effective means of obtaining information than one of the techniques which does.

181. In considering an application for a warrant to use two or more methods, the Federal Court Judge would have to consider the strength of the case which is made for the necessity of using each technique. He should also be informed, when considering any application, whether warrants have been issued for the use of other techniques in relation to the same subject of investigation and, if they have, what results they have produced. It is essential that the judge be in a position to consider whether, given what has been obtained or what can

reasonably be expected to be obtained from other techniques, and given the statutory direction to minimize intrusions on privacy, the necessity of using a particular technique has been demonstrated.

182. Finally, an important focal point in the review of the warrant process carried out by the Parliamentary Committee and the Advisory Council on Security and Intelligence would be the extent to which the various warrants are used together. Indications that warrants were being applied for and obtained on a 'blanket' basis would justify a critical re-examination of the system.

183. The system of judicial warrants we have proposed would require the repeal of section 16 of the Official Secrets Act and its replacement by provisions of the statute governing the security intelligence agency. We have set out below a draft of the legislative provisions we envisage for this purpose.

Proposed Section of the National Security Act

(1) In this section,

(a) "interception" includes listening to, recording or acquiring any communication, any written communication other than a message in the course of post, and any telecommunication, and acquiring the substance, meaning or purport thereof;

(b) "premises" includes any land, place, vehicle, trailer, mobile home, vessel or aircraft.

(2) Upon the application of the Director General of the Security Intelligence Agency approved in writing by the Solicitor General of Canada, a designated judge of the Federal Court of Canada may issue a warrant authorizing one or more of the following:

(a) the interception or seizure of any communication, other than a message in the course of post, by the use of an electromagnetic, acoustic, mechanical or other device;

(b) the interception or seizure from any person having, in the ordinary course of business, custody of the original copy, record or transcript of any communication, other than a message in the course of post;

(c) the operation of a concealed optical device or camera in a place to which the public does not have access;

(d) the use of a dial digit recorder;

(e) in respect of an article of mail in the course of post, an examination of its exterior, photographing of its exterior, or its opening and the examination and copying of its contents;

(f) the inspection of any premises and of any specified thing or things generally to be found in the premises, and the photographing or copying of the thing or things;

(g) access to personal information (other than biographical information as defined in this Act) under the control of government institutions.

(3) Before issuing a warrant under subsection (2) the judge must be satisfied by evidence on oath that the procedure authorized is necessary for the prevention or detection of any of the following activities:

(a) activities directed to or in support of the commission of acts of espionage or sabotage ('espionage' and 'sabotage' to be given the meaning of the offences defined in sections 46(2)(b) and 52 of the Criminal Code and section 3 of the Official Secrets Act);

(b) foreign interference, meaning clandestine or deceptive action taken by or on behalf of a foreign power in Canada to promote the interests of a foreign power;

(c) political violence and terrorism, meaning activities in Canada directed towards or in support of the threat or use of serious acts of violence against persons or property for the purpose of achieving a political objective in Canada or in a foreign country.

(4) An applicant for a warrant must disclose to the judge before whom the application is brought the details of any application made previously with respect to the same matter.

(5) In deciding whether the procedure for which such authorization is applied for is necessary for the prevention or detection of any such activity, the judge shall take the following factors into consideration:

(a) whether other investigative procedures not requiring a judicial warrant have been tried and have failed;

(b) whether other investigative procedures are unlikely to succeed;

(c) whether the urgency of the matter is such that it would be impractical to carry out the investigation of the matter using only other investigative procedures;

(d) whether, without the use of the procedure it is likely that intelligence of importance in regard to such activity will remain unavailable;

(e) the value of the intelligence product obtained from any warrants previously issued pursuant to this Act in relation to the same subject of investigation;

(f) whether the degree of intrusion into the privacy of those affected by the procedure is justified by the value of the intelligence product sought;

(g) such other circumstances as may be relevant.

(6) The Director General of the Security Intelligence Agency may, with the written approval of the Solicitor General, appeal a refusal of a judge to grant a warrant to the Federal Court of Appeal.

(7) In emergency situations where, in the opinion of the Solicitor General of Canada, the time required to bring an application before a judge would result in the loss of information necessary for the protection of the security of Canada, the Solicitor General of Canada may issue a warrant to the Director General authorizing the use of one or more of the procedures listed in subsection (2) for a period of 48 hours, provided that he is satisfied by evidence on oath that it is necessary for the purposes set out in subsection (3) and provided that the warrant is subject to the same terms and conditions other than the maximum time periods that would apply if a warrant for the same purpose was issued under subsection (2). The Advisory Council on Security and Intelligence must be notified whenever a warrant is issued under this subsection.

(8) A warrant issued pursuant to subsection (2) or subsection (7) shall be issued to the Director General and those persons who act upon his direction or with his authority and

(a) in the case of a communication, shall specify the type of communication to be intercepted or seized;

(b) in all cases, shall state the activity referred to in subsection (2) in respect of which the warrant has been applied for;

(c) in all cases, shall specify the length of time for which the warrant is in force, which shall not exceed 180 days;

(d) in all cases, the judge by whom the warrant is issued or the Solicitor General issuing a warrant under subsection (7) shall include therein such terms and conditions as he considers appropriate, including such powers as are provided for in subsection (9) and are appropriate in order to enable the procedure to be effected without the knowledge of any unauthorized person.

(9) A warrant issued pursuant to subsection (2) or subsection (7) may provide that in the case of the procedures referred to in (a), (b), and (f) of subsection (2) the persons carrying out the procedure may take such steps as are reasonably necessary to enable them

(a) to install any device the use of which is authorized;

(b) to monitor, repair and remove the device;

(c) to enter premises for the purpose of

(i) examining the premises prior to installation of the device;

(ii) installing the device;

(iii) monitoring, repairing and removing the device;

(d) to operate the device by using the electrical power supply that is available in the premises;

(e) to copy material;

(f) to examine the contents of receptacles, including luggage;

(g) to take such other steps as may be reasonably necessary for such purpose,

provided always that in all these cases

(h) any such steps shall cause no significant damage to the premises that remains unrepaired; and

(i) in no case shall the persons carrying out the procedure use physical force or the threat of such force against any other person; and

(j) in every case the persons carrying out the procedure shall be accompanied by a peace officer.

(10) (a) The Postmaster General of Canada shall be notified whenever a warrant is issued pursuant to subsection (2) or subsection (7) authorizing use of the procedure referred to in (e) of subsection (2), and Canada Post shall give to persons acting in pursuance of such a warrant all reasonable assistance.

(b) A warrant issued pursuant to subsection (2) or subsection (7) may provide that in the case of the procedures referred to in (e) of

subsection (2) the persons carrying out the procedure may remove the article of mail from the course of post and even from the post office but only as long as is reasonably necessary to enable the procedure which is authorized to be carried out.

(c) The procedure authorized by such a warrant may be carried out notwithstanding the provisions of section 43 of the Post Office Act and without any person thereunto duly authorized committing any offence under that Act.

(11) Warrants issued pursuant to subsection (2) and subsection (7) authorizing the use of the procedure referred to in (g) of subsection (2) shall be submitted to the head of the government institution which controls the information which is requested and the head of the institution shall direct that the information requested be disclosed according to the terms specified in the warrant.

(12) A renewal of the warrant may be given if the judge to whom an application for the renewal is made is satisfied that, if the application were for a warrant, he would have issued it pursuant to subsection (2), and, in addition to the requirements of subsections 3, 4 and 5, he shall be provided with evidence under oath as to the intelligence obtained pursuant to the warrant.

(13) The Solicitor General of Canada shall, as soon as possible after the end of each year, prepare

(a) a statistical report to be laid before Parliament setting forth

(i) the number of warrants issued for each of the procedures referred to in (a) to (g) of subsection (2);

(ii) the number of warrants issued which were renewals of warrants previously granted;

(iii) the extent to which warrants have been renewed more than once.

(b) a report to be presented for examination by the Joint Committee of Parliament on Security and Intelligence providing

(i) an assessment of the value of the intelligence products resulting from the use of warrants issued under subsection (2);

(ii) an account of any difficulties encountered in the administration of this section which might indicate the need for amendments to the section.

(14) Section 178.11(1) of the Criminal Code shall not apply to

(a) a person who intercepts a private communication as defined in section 178.1 in accordance with a warrant issued pursuant to subsection (2);

(b) any person who in good faith aids in any way a person who he has reasonable and probable grounds to believe is acting under the authority of any such warrant.

(15) Section 178.18(1) of the Criminal Code shall not apply to a person in possession of a device such as is referred to therein for the purpose of using it in an interception made or to be made in accordance with a warrant issued pursuant to subsection (2).

(16) Section 178.2(1) of the Criminal Code shall not apply to a person who discloses a private communication, as defined in section 178.1 of

the Criminal Code, or any part thereof or the substance, meaning or purport thereof or of any part thereof, or who discloses the existence of a private communication for any purpose within the scope of the power of the security intelligence agency, or for any purpose of review of the operation of this section exercisable pursuant to this Act by the Advisory Council on Security and Intelligence and the Parliamentary Committee on Security and Intelligence.

(17) No action lies under Part I.1 of the Crown Liability Act in respect of any procedure carried out pursuant to a warrant issued under subsection (2).

(Section 16 of the Official Secrets Act would be repealed. The new section should provide for the continuation in effect of all warrants issued under section 16 of the Official Secrets Act for 30 days after the coming into effect of the section, as if they had been authorized by a warrant issued by a judge pursuant to the new section.)

(Section 178 of the Criminal Code should be amended wherever necessary to ensure that an interception under a warrant is on the same plane as one pursuant to a section 178 authorization: e.g. to ensure that there is no question about the admissibility of the intercepted private communication in evidence in a judicial proceeding.)

CHAPTER 5

ANALYSIS, REPORTING, AND ADVISING FUNCTIONS

INTRODUCTION

1. In previous chapters in this part of our Report, we established criteria for deciding the proper subjects or targets of a security intelligence agency's investigative activities. We also described the methods that the agency can employ to collect information about these targets, and the controls necessary to ensure that the risk to Canada's security justifies the use of the more intrusive means of gathering information. In this chapter, we focus on what the agency should do with the information it collects. We begin with the analysis function by examining the purposes of analysis and the current strengths and weaknesses of the Security Service's analytical capabilities. Our recommendations for improving this function then follow. A fundamental theme throughout this section is our belief that analysis is of prime importance for a security intelligence agency which is effective and which acts within the law. Indeed, it is not an exaggeration to say that analysis has a dominant effect on all of the significant activities that such an agency performs.

2. From analysis, we turn to the agency's reporting and advising functions. We begin by developing basic principles in regard to two matters: first, what the agency should report and advise on, and second, to whom it should report and give advice. We then describe the nature of the reporting and advising programmes that a security intelligence agency should adopt and conclude with recommendations on the type of controls which should govern the reporting function.

A. ANALYSIS

The importance of analysis

3. Those familiar with security or intelligence agencies often describe the work of these organizations in terms of four functions: targetting, collecting, analyzing, and dissemination (Vol. 69, pp. 11180-82). We have found this description useful for some purposes, including the structuring of this part of our Report. Nevertheless, the simplicity of this description, though one of its attractive features, may lead to difficulties if it is used as a basis for drawing important conclusions about organizing the government's security intelligence functions. For example, to conclude that any of the four functions is a separate

component which can be neatly detached from the others and placed in a separate organization would be a serious misjudgment.

4. That is why we disagree with Commissioner Simmonds, who, in his testimony before us, suggested that the R.C.M.P. Security Service should become essentially a collection agency, and that primary responsibilities for analysis should lie elsewhere in government:

> . . . if for the future we take a look at a different way, in broad terms, of Government organization to handle security matters, then it seems to me that the role of the Service within the Force should be mostly one of just investigating and collecting intelligence and so on and doing low level analysis, but some of the things we, perhaps, have been expected to do, be done in another forum.
>
> (Vol. 165, p. 25377.)

The most compelling reason for rejection of that opinion is that a security intelligence agency cannot do the targetting and collecting functions properly and effectively without a well-developed analytical capability. The judgments involved in the targetting process are difficult. When, for example, does proper diplomatic behaviour shade into foreign interference? What forms of political violence are properly the concern of a security intelligence agency in addition to being the concerns of local and provincial police forces? What is the difference between 'revolutionary subversion' and dissent? Such judgments should be based on more than 'low level' analysis.

5. There is a similar need for sound analytical skills in directing the agency's investigative work. Those in senior operational roles are required to make important choices daily about the allocation of the agency's limited investigative resources: whether, for instance, physical surveillance teams should follow target A or target B to ensure the likelihood of the bigger payoff, and when it is appropriate to use other investigative tools, including electronic surveillance and informants. After information about a target is collected, agency personnel must analyze it so as to redirect investigative efforts if necessary. This type of analysis involves the piecing together of scraps of information to produce a working hypothesis about the intentions and plans of the target. Intuition, experience in the tradecraft of counter-espionage, and knowledge of the target combine with clear logical analysis to produce expertise in this area. Without such expertise, a security intelligence agency cannot possibly be successful in its investigative work.

6. Analysis plays a key role in the agency's reporting function. Raw information about possible threats to security will be of little value to government unless the significance of that information is explained clearly. Crucial to this reporting function is the capacity of agency personnel to undertake research using books, articles and reports on all subjects related to the social, economic, and political processes — national and international — relevant to the security of Canada. This research is important not only in writing reports to government but in distinguishing between those activities which require surveillance and those which do not.

7. Another argument bolsters our conclusions about the importance of analysis to a security intelligence agency. Any other department or agency would have difficulty in getting access to the kind of information collected by the security agency, and therefore would have difficulty in attempting analysis. In evidence before us, Mr. Robin Bourne, the former head of the Police and Security Planning Branch in the Solicitor General's Department, made this point as follows:

> The first problem was the whole business of the need-to-know information and protecting third party interests. Obviously, long-term research into these kinds of subjects would not be effective, unless we had all the information that was available to do this kind of research. There is no question that we were not getting from the R.C.M.P., which was the prime source, all the information which we needed to have for that kind of research... and there were very good reasons for that...
>
> Everyone is suspect in the security business until they prove themselves otherwise. We hadn't really had time to prove ourselves. So, we really did not have the basic information to do the research... I think you will find that throughout the world, most security services and intelligence organizations do have as an integral part of their organization, the research branch, just for that reason. So that they do have free access to the information.
>
> (Vol. C68, pp. 9471-73.)

With regard to Mr. Bourne's first point, our examination of the R.C.M.P. files concerning the relationship between the Security Planning and Analysis Research Group (SPARG) and the Security Service satisfies us that the Security Service will vigorously resist any proposed arrangement that would involve outside analysts having access to Security Service files.

8. To recognize the importance of analysis, the security intelligence agency's analytical responsibilities should be stated explicitly in the statute establishing the agency. This is not to argue that the analysis function should reside exclusively with the security intelligence agency. Rather, a number of agencies should have skills in this area. The question then becomes how these skills are co-ordinated at the centre of government to be of maximum benefit to Ministers and senior government officials. We shall return to this question in Part VIII of this Report, where we discuss the security and intelligence co-ordination mechanisms at the centre of government.

Assessing the Security Service's analytical capacity

9. The Royal Commission on Security in 1969 was critical of the Security Service's capacity to provide government with clear, timely, useful information about security threats facing Canada.

> Although the role of the R.C.M.P. is admittedly ill-defined, and recognizing that government policy has been inhibiting, we are not sure that the R.C.M.P. has made a sufficient, or a sufficiently sophisticated, effort to acquaint the government with the dangers of inaction in certain fields. We are left with the impression that there has been some reluctance on their part to take desirable initiatives and some inadequacy in stating the case for necessary security measures in interdepartmental discussions at the higher policymaking levels. A specific area in which the effectiveness of the

R.C.M.P. does appear to us to be capable of improvement involves personnel investigations.[1]

10. Our own research — based on interviews with Security Service personnel and the primary consumers of Security Service intelligence reports in other government departments, and based on a thorough study of a cross-section of Security Service reports — leads us to conclude that, while there has been some improvement since the Royal Commission on Security, the Service still has serious deficiencies in this area. One of our findings is that the Security Service's reports and assessments are heavily oriented to providing covertly collected information about specific groups and individuals. Many departments which receive these reports have found them useful and have complimented the Service on its investigative skills. Reaction to Security Service products, however, has been by no means uniform. Officials of several departments have been highly critical, voicing two common complaints: Security Service personnel lack experience and knowledge about what constitutes legitimate diplomatic behaviour, and they do not know enough about government — how it works and the needs of Ministers. Our review of Security Service reports confirmed the validity of these criticisms, and indeed, many within the Security Service agree with them. We, as a Commission, add an additional concern. Some of the analysis done by the Security Service demonstrates a serious inability to distinguish between agitators for social change and those who pose a significant threat to Canada's democratic process of government. Examples of this tendency occurred in the work done on the Extra Parliamentary Opposition (E.P.O.), and in the analysis leading up to the countering operations in the early 1970s (Operation Checkmate).

11. The Security Service is weakest when it comes to analysis which is longer term, more broadly based, and less oriented to specific groups and individuals. Such analysis, which tends to rely on both overt and covert sources of information, is often called 'strategic' analysis. The Security Service does not do enough of this type of analysis and what it does is not of high quality. In voicing this criticism we are not arguing that the Security Service lacks potential in this area: we have met a number of Security Service staff with well-developed analytical talents. The problem is that there are not enough of them and, in addition, those in middle management often lack the skills and experience to supervise them properly.

12. Some Security Service members have argued vigorously that strategic analysis is not within their mandate: they have not been asked by government to perform this function. We believe that such an argument is based on too narrow an interpretation of the Security Service's mandate. The argument is also suspect in that the Security Service has, on occasion, done just this broader based, longer term type of analysis. The chief reason why the Security Service does so little of this type of analysis, in our view, is that its members do not feel confident about their capacity for doing it. As a result, Security Service products are often unbalanced, relying far too much on covertly collected information, and not nearly enough on what is available through overt means.

---

[1] *The Report of the Royal Commission on Security*, paragraph 56.

Proposals to strengthen the analytical function

13. Our proposals for strengthening the analytical capabilities of Canada's security intelligence agency fall into three categories. First, we shall recommend in Part VI, Chapter 2, that the agency be staffed with individuals who are well-educated in a variety of disciplines, who express themselves clearly, who have in many instances working experience in other organizations before joining the agency and who are full members eligible for promotion to senior positions. Similarly, the agency requires senior and middle level managers who can select, develop, and direct a highly versatile and well-educated staff. Second, in Part VIII, Chapter 1, we shall recommend a revamped and revitalized interdepartmental committee system, which will allow the consumers of the agency's products to play a more active role in setting the government's intelligence collection priorities and in providing the collecting agencies with better assessments of the strengths and weaknesses of their current products. Third, also in Part VIII, Chapter 1, we shall recommend that the government establish a central Bureau of Intelligence Assessments to provide intelligence estimates derived from the products of collecting agencies and from public sources of information. Such a bureau, we believe, should develop a small but highly expert staff to serve, in part, as a stimulus to other security and intelligence agencies within government to improve the quality of their analyses. In addition to these proposals, we shall put forward, as a suggestion only, an organizing approach to ensure that those specializing in analysis within the security intellligence agency are used with most benefit. We now turn to this suggestion.

14. On two separate occasions in the past, the Security Service established a specific unit, separate from the operational branches, with the resources and responsibility for doing research and analysis. The disadvantage has been that such a unit tends to get cut off from the operational branches. 'Hardnosed' operational personnel view these intellectually oriented researchers with suspicion, are reluctant to share their most sensitive information with them, and resent having their conclusions 'reworked' by a group without any current operational know-how. The result is that the separate research group works primarily on peripheral matters, and the overall quality of analysis has not been improved to any degree. Another solution, which the Security Service has also tried, is to establish separate analytical units within each operational branch. The risk in this approach is that these units will focus entirely on high priority operational problems and have little time for more in-depth contextual analysis and research.

15. One way out of this dilemma which we believe worthy of consideration is to establish a small research group which does not formally report to any of the operational branches but is available to them as a centralized service. Operational branches would retain responsibility for producing major pieces of analysis (requests for these papers would likely come from interdepartmental committees or the senior management of the agency), and would second researchers and writers for short periods from this central pool to work with their operational people for this purpose. Such temporary working groups within the agency would bring together the writing skills and familiarity with

overt sources which the centralized pool of researchers would possess, with the 'street' knowledge and access to covert sources of information which are the forte of those in operational branches.

WE RECOMMEND THAT the security intelligence agency's responsibilities for the development of a competent analytical capability be explicitly stated in the statute establishing the agency.

(28)

B. REPORTING AND ADVISING

Basic principles

16. The reporting of timely, cogent information about security threats facing Canada is the *raison d'être* of a security intelligence agency. The word "dissemination" is often used by those working in security and intelligence organizations as a convenient label for this function, but we prefer the term "reporting". "Disseminate", according to The Concise Oxford Dictionary, means "scatter about, sow in various places". In our examination of Security Service reporting activities, we have found evidence of numerous problems stemming from poor judgment concerning both what the Security Service reports and to whom. In our view, there should be no indiscriminate spreading of security intelligence information, especially information relating to individuals and groups. For this reason, we prefer to use the word "reporting".

17. Given the importance of the reporting function, it should be provided for in the Act establishing the agency. In addition, the Act should state that limits must be applied to this reporting function in the form of instructions or guidelines issued by the Minister responsible for the security intelligence agency. These guidelines should be approved by the Cabinet Committee on Security and Intelligence and reported to the Joint Parliamentary Committee. We briefly set out here a number of principles on which these guidelines should be based.

18. The first of these principles is that the security intelligence agency, with few exceptions, should report only information relevant to threats to security as those threats have been defined by Parliament. The agency should not report information which names individuals or groups, unless such information can reasonably be related to some activity threatening the security of Canada. Information concerning individuals should be reported only to departments which require it for security clearance purposes or to departments, Ministers, police forces or foreign agencies who need the information because of their recognized responsibilities to deal with security threats as defined by the Canadian Parliament. In Chapter 7 of this Part we shall discuss the types of problems which a security intelligence agency can encounter in reporting information to foreign agencies. We shall also suggest control procedures for governing this activity.

19. In enunciating the above principle, we have purposely inserted the qualifying phrase "with few exceptions". This qualification is meant to cover those few cases where the security intelligence agency, in the course of

investigating a threat to security as defined by Parliament, *accidentally* comes across information unrelated to the security of Canada which it should report to a domestic police force, or to a provincial government or to the federal government. For example, in its investigations of a domestic group suspected of plotting some terrorist act, the security intelligence agency may stumble upon information about activities which, though criminal, are unrelated to national security. We believe that the security intelligence agency must report such information to the appropriate police force. If the agency believes that to report such information would likely be detrimental to the security of Canada, full details of the matter should be reported immediately to the Solicitor General, for his decision as to whether or not the information ought to be reported. While we think it desirable that the Solicitor General should consult with the Attorney General of Canada at this stage, he should not be obliged to do so if he believes that the information ought to be released to the police. On the other hand, if the Solicitor General agrees that the security of Canada would be adversely affected by reporting the matter to the police, he should refer all the details to the Attorney General of Canada for his decision as to whether the interests of the security of Canada outweigh the interests of the administration of justice. (See discussion in Chapter 8 of this Part.) As a second example, if the security intelligence agency, in its investigation of a suspected foreign intelligence officer, were accidentally to collect information relating to a foreign government's prospective bargaining position on an important trade issue with Canada, we believe it should be able to report such information to the appropriate Federal or Provincial government department.

20. We recognize that, in allowing exceptions to the general principle about reporting only security relevant information, we open up a potential for two kinds of abuse. First, if the agency is permitted to report information which it has no mandate to collect, there is a great danger that its collection activities will secretly expand. Second, there is a danger that the agency will report certain accidental by-products which it has no business reporting. For example, it would be highly improper for Cabinet Ministers to receive information about their political opponents from a security intelligence agency. Using the agency in this manner would do irreparable harm to Canada's democratic form of government. Similarly, a security intelligence agency should not report any information it has collected accidentally on the policies or strategy of a provincial government.

21. To guard against these potential abuses, we make several proposals. As a first step, the ministerial guidelines on reporting should deal explicitly with the types of accidental by-products of authorized investigations which the security intelligence agency can properly report. Before reporting these by-products, the agency should require ministerial approval. In addition, the security intelligence agency should retain, in one convenient location, records of all accidental by-products reported to government or to the police so that the independent review body has ready access to them. These records should state what information was reported, how the reported information was collected, to whom it was given, and the history of the investigation which produced the information. The independent review body should monitor closely these investi-

gations to ensure that they are not being misdirected for a purpose irrelevant to the security of Canada. Finally, the security intelligence agency should not analyze the accidental by-products, nor should it comment on their significance.

22. In addition to elaborating upon the type of information that a security intelligence agency can report, the guidelines issued by the Minister should also make clear to whom the agency can report information. Ministers, both provincial and federal, government departments, police forces, and foreign agencies will be the chief recipients of the products produced by the agency. The agency, however, should not report information on its own initiative directly or indirectly to the news media. As we state in the next chapter on executive and preventive functions, it should not be the responsibility of the agency to publicize threats to security. That function must rest with the Minister responsible for the agency. There should be no contrived 'leaks' by the security intelligence agency nor cultivation of media sources for the purpose of planting articles provided by the agency. Activity of this kind is highly dangerous in that it may involve the agency in attempts to manipulate the media.

23. The agency should also exercise great care in reporting information to individuals who are not government officials, Ministers, or police officers. In the chapter which follows, we shall discuss when it is proper for a security intelligence agency to do so.

24. There is one additional topic concerning the reporting function which we wish to address. That focusses on the caution practised by a security intelligence agency in revealing the sources on which its intelligence judgments are based. Policymakers can find such caution frustrating if they wish to know whether the agency's judgments are based on information provided by a strategically placed agent, on inference drawn from diverse pieces of information, or simply on a guess on the part of the agency analysts. On the other hand, an agency's reticence in these matters is not entirely without foundation. Consider the following example documented by an American author writing about the C.I.A.:

> With war raging in Bangladesh between Indian and Pakistani forces in December 1971, evidence began to mount that India was planning an attack on West Pakistan as well. On December 7, Kissinger asked the C.I.A. for an estimate of the probability of such an attack. The C.I.A. said it didn't know. But within twenty-four hours it had positive information: the C.I.A. case officer handling the Indian politician in Gandhi's cabinet in New Delhi was told that a decision had just been reached to attack in the West. A report was immediately cabled back to Langley and forwarded directly to the White House in its raw form. Nixon was later to cite this cable as one of the few really timely pieces of intelligence the C.I.A. had ever given him, but the Agency paid a price. The report was widely read in the White House, and its text, along with many other documents, was quickly leaked to Jack Anderson, who published them in his column in mid-December. That was the end of the agent. According to [a senior C.I.A. intelligence officer], "he told us to go to hell".[2]

[2] Thomas Powers, *The Man Who Kept the Secrets*, New York, Alfred A. Knopf, 1979, pp. 206-207.

25. The dilemma described above is not unique to the United States. During interviews conducted by members of our research staff, several officials from 'consumer' departments complained about the Security Service's refusal to divulge its sources. For example, officials from one department cited two occasions when the Security Service attempted to get the Intelligence Advisory Committee's approval for assessments which some members of the Committee strongly suspected came from foreign intelligence services. While this dilemma about revealing sources is not fully resolvable, the security intelligence agency should enter into discussions with consuming departments about how it can best reveal the basis for its judgments while providing reasonable protection for its sources. We believe that a security intelligence agency should be able to provide at least a general idea of the nature of its sources on which a particular report is based, i.e. whether the sources are domestic, foreign, or a combination and the number and reliability of these sources. The Minister responsible for the agency should also address this question in his guidelines on the reporting function.

Reporting and advising programmes

26. Our review of security intelligence reporting activities has revealed that the Security Service produces a large number of reports. These reports are distributed to a wide variety of consumers from the Prime Minister in some instances to Departmental Security Officers in others. As mentioned earlier, a large majority of these reports tend to be case-oriented, that is, they tend to deal with information collected by covert means about specific groups and individuals. Our recommendations concerning the proper mandate of a security intelligence agency ensure that security intelligence products will continue to be numerous and to be read by a wide variety of consumers. Nonetheless, there should be several important changes. Security intelligence reports should put more emphasis than is now the case on providing government with timely advice on such matters as crisis handling and protective security. In addition, security intelligence reports should be less case-oriented: greater attention should be paid to providing government with longer term, more broadly based assessments of security threats facing Canada. Furthermore, the security intelligence agency's reports to government officials and Ministers about specific groups and individuals should make greater efforts to put this information in context. Thus, a report on the activities of a suspected foreign intelligence officer may need to make clear the difference between acceptable and unacceptable diplomatic behaviour and how the intelligence officer's activities might relate to his country's foreign policy. We will elaborate on these themes further in our discussion of the major security intelligence reporting and advising programmes in the following four areas: screening, emergencies and crises, protective security, and reporting on security threats.

Security screening

27. Our recommendations for the security intelligence agency's role in security screening — recommendations which we shall develop in Part VII of this Report — call for a significant change in the reporting responsibilities of the agency, especially with regard to screening for government appointments. We

shall propose that the agency no longer have responsibility for doing routine field investigations on all Top Secret clearances. In addition, the agency should report only information on an individual's character which is of direct relevance to security. The effect of these recommendations and others calling for a reduction in Top Secret clearances will dramatically reduce the number of routine reports that the Security Service now provides departmental security officers. However, other recommendations concerning screening for government appointments will increase the agency's advisory responsibilities. For example, we shall recommend that the agency develop a competent research capacity for the purpose of providing advice to government on a variety of matters relating to subornation of public servants, including the following: the latest techniques used by foreign intelligence officers to compromise people; the risks posed by individuals with certain character traits; developments relating to security screening in other countries; and possible policy changes to improve the government's screening procedures. Thus, the changes in screening responsibilities, at least in the public service area, call for a shift away from routine reports on individual cases to more emphasis being placed on providing policy advice to government.

Emergencies and crises

28. In Part IX, Chapter 1, we shall discuss the role of a security intelligence agency in emergencies and crises. After describing the role played by the Security Service in the 1970 October Crisis, we shall emphasize the importance of the ability of a security intelligence agency to provide opportune, well-written reports which warn governments of potential crises and, in turn, of the capacity of government to digest these reports and react to them. The number as well as the content of such reports calls for careful judgment. Too many reports will lead to officials and Ministers ignoring the agency's advice on these matters. Similarly, the government will lose confidence in the agency if it is too cautious in forewarning about significant political violence. In addition to advising on potential crises, the security intelligence agency should provide government with periodic reports on crisis-handling. The agency should be knowledgeable about the latest trends in international terrorism, the changing nature of terrorist goals and targets, and, among other things, the steps being taken by various foreign governments to counter terrorist threats. In our opinion, the R.C.M.P. Security Service does far too little of this type of reporting to government.

29. The agency also has an important reporting role during a particular crisis. It will be responsible for providing the federal government's crisis centre with accurate, up-to-date intelligence reports based on information received from police forces, foreign agencies, and other government departments. Thus, the agency has a filtering function which requires careful judgment and communication skills so that the crisis centre is neither confused by conflicting reports from several sources nor denied an essential piece of information originating from other agencies.

Advice on protective security

30. A security intelligence agency should be a major source of advice to government departments and police forces which are responsible for enforcing and carrying out measures to protect property and persons from security threats as defined by Parliament. The agency itself should not be assigned the task of actually enforcing or carrying out protective security functions. For example, in airport policing, the agency's role should be to provide information about terrorist threats to airport security officials, to the police and to the Ministry of Transport. In V.I.P. security, the agency should provide intelligence about those who are likely to attack V.I.P.'s for political purposes — their identity, whereabouts and methods. In the vital points programme, the role of the security intelligence agency should be to report on the kinds of situations in which vital points might be attacked by those who fall within the agency's mandate, and on the basis of this analysis, to assist those responsible for the vital points programme in identifying vital points and designing effective security measures. The emphasis in all of these areas, therefore, is on providing useful information and advice, and not on actually carrying out security programmes. Once again, it is our view that the Security Service does not provide government with enough high quality advice on these matters.

Reporting on security threats

31. Throughout the year, the Security Service provides government with reports on a wide variety of security threats which may not have a direct relationship to screening, preparing for crises, or providing protective security. Some of these reports are provided on a regular basis. For example, the Security Service is required by the 1975 Mandate to report annually to Cabinet. Other reports result from priorities set by an interdepartmental committee. For example, the Intelligence Advisory Committee has, on occasion, requested that the Security Service co-operate with other departments in producing a report canvassing the covert operations in Canada of a particular country. Many of the Security Service's reports, however, result from *ad hoc* requests from departments for information about a particular group, individual, or upcoming event. All such *ad hoc* requests for information from departments or police forces should be drawn to the attention of the agency's headquarters staff to ensure that investigations resulting from these requests are subject to the regular control procedures.

32. Earlier in this chapter, we proposed that the agency place more emphasis on providing government with reports on the strategic aspects of security threats facing Canada — how these threats are changing, and the measures government might take to deal with them. In subsequent parts of this Report, we shall make additional recommendations affecting this aspect of the agency's reporting responsibilities. In Part VIII, we shall make proposals for how the agency might improve its annual report to Cabinet. We shall also be recommending that the function of collating and assessing current foreign and security intelligence be consolidated in the Intelligence Advisory Committee. This change will likely affect the current practice of the Security Advisory Committee in preparing and circulating a weekly security intelligence report.

Finally, our recommendation calling for the establishment of a Bureau of Intelligence Assessments should have an important impact on the reporting functions of the security intelligence agency. The agency will find itself responding to many more requests than at present to participate in interdepartmental teams established to assess a variety of longer term security problems facing Canada.

33. In conclusion, the recommendations in this Report have important implications for the reporting and advising programmes of a security intelligence agency. Future emphasis will be placed more on providing its consumers with advice and analysis on security problems and less on routine reports dealing with specific individuals and groups.

Controls on the reporting function

34. We conclude this chapter by summarizing briefly the system of controls which should govern the security intelligence agency's reporting function. This system should consist of at least four parts. The first is the set of guidelines which the Minister responsible for the agency should issue under the authority of the Act creating the agency. The Minister should disclose these guidelines to the Joint Parliamentary Committee. As we noted earlier in this chapter, these guidelines should cover at least the following topics:

— conditions under which the agency can report information about individuals;

— conditions under which the agency can advise individuals outside of governments and police forces about security threats;

— the types of information not relevant to its mandate which the agency, having collected by accident, can report to government;

— the manner in which the agency should handle *ad hoc* requests for information from government departments and police agencies; and

— the manner in which the agency should reveal the basis for its judgments, while at the same time providing reasonable protection for the sources of its information.

We shall also recommend that the Minister responsible for the agency issue guidelines with respect to the agency's relationships with foreign agencies. These guidelines will also be relevant to the agency's reporting function.

35. The second aspect of the system of controls governing the reporting function will be the independent review body — the Advisory Council on Security and Intelligence — which we shall recommend in Part VIII. This advisory body will monitor the security intelligence agency's operations including its reporting activities, and in this regard, will be an *ex post facto* control. In performing this function, the Minister's guidelines referred to above will be an invaluable aid in determining those areas of the agency's work which require the Advisory Council's close attention. Complaints by members of the public and by agency employees will be other means whereby this advisory council can direct its investigations.

36. Another *ex post facto* control on agency reporting will be the Security Appeals Tribunal which we shall recommend in Part VII. This Tribunal will handle all complaints concerning the federal government's screening activities regarding public servants, immigrants and applicants for Canadian citizenship. Thus, the tribunal will be an important review mechanism for information reported by the agency on individuals.

37. A final element in the control system governing the agency's reporting function will be a revamped interdepartmental committee system which we shall recommend in Part VIII. The departments and agencies within the federal government which are the principal customers of intelligence reports have not in the past played a sufficiently active role in the process of setting priorities for those organizations, including the security intelligence agency, which collect and report security and foreign intelligence. A more active group of consumers is essential if the government hopes to achieve value for its money in this area.

WE RECOMMEND THAT the Act establishing the security intelligence agency specify the reporting function of the agency and require the Minister responsible for the agency to issue guidelines on how the agency should conduct its reporting activities. These guidelines should cover at least the following:

(a) conditions under which the agency can report information about individuals;

(b) conditions under which the agency can advise individuals outside governments and police forces about security threats;

(c) (i) the general principle that the security intelligence agency should report only information relevant to its mandate, except that information which it has collected by accident which the guidelines specifically require or authorize it to report to government or to the police;

(ii) the agency should report information which it has collected by accident, which relates to an offence, to the appropriate police force if, in the agency's opinion, to do so would not be likely to affect adversely the security of Canada.

(iii) the types of information collected by accident which the security intelligence agency may report to the appropriate federal or provincial government include information pertinent to the economic interests of Canada.

(d) the manner in which the agency should handle *ad hoc* requests for information from government departments and police forces;

(e) the manner in which the agency should reveal the basis for its judgments, while at the same time providing reasonable protection for the sources of its information.

(29)

WE RECOMMEND THAT when the Solicitor General receives information from the security intelligence agency relating to the commission of an offence, and the agency considers that it would adversely affect the security of Canada to pass that information to the police, the Solicitor

General should consult with the Attorney General of Canada with respect to the release of that information. If, after such consultation, the Solicitor General decides that the security of Canada would not be adversely affected by the release of that information he should instruct the agency to release it to the appropriate police force. On the other hand, if the Solicitor General decides that the release of the information would adversely affect the security of Canada, he should so advise the Attorney General of Canada who should proceed in accordance with arrangements to be worked out with provincial attorneys general. (See discussion in Chapter 8 of this Part.)

(30)

WE RECOMMEND THAT

(a) the security intelligence agency retain, in one location, records of all accidental by-products reported to government or to the police, and that such records state what information was reported, how the information was collected, to whom it was given, and the history of the investigation which produced the information; and,

(b) the independent review body have access to such records and that it monitor closely the investigations which produced the information to ensure that the investigations are not being misdirected for a purpose irrelevant to the security of Canada.

(31)

WE RECOMMEND THAT the agency, in addition to providing information about specific individuals and groups relevant to its mandate, place greater emphasis than is now the case on providing government with:

(a) analysis and advice on the latest developments, techniques, and countermeasures relating to physical and V.I.P. security, and security screening; and,

(b) reports which analyze broad trends relating to threats to the security of Canada and which advise government on ways to counter these threats.

(32)

CHAPTER 6

EXECUTIVE POWERS AND PREVENTIVE ACTIVITIES

INTRODUCTION

1. Because the essential function of a security intelligence agency is to collect, analyze and report intelligence about threats to Canada's security, we believe it should not be authorized to enforce security measures. Thus, we think the statutory mandate of the agency should not include the functions of "deterring, preventing and countering" which are now included in the 1975 Cabinet Directive defining the Role, Tasks and Methods of the R.C.M.P. Security Service.

2. We have two basic reasons for taking this position. First, as we argued in Part III, we think it is unacceptable in Canada that the state should use a secret intelligence agency to inflict harm on Canadian citizens directly. This position, it must be noted, does not prevent a police force or a government department from using intelligence supplied by the security intelligence agency to enforce a law or security measure against an individual. Second, we think the liberty of Canadians would be best protected if measures to ensure security were not enforced by the organization with the prime responsibility for collecting information about threats to that security. The assignment of executive enforcement responsibilities to agencies other than the security intelligence organization assures desirable countervailing powers and avoids the danger that the security intelligence organization might be both judge and executor, in security matters.

3. Therefore, we think it would be wise to separate the enforcement function. In this Canada would be following the Australian and New Zealand examples of expressly excluding enforcement functions from the authorized activities of the security intelligence agency. The Australian Security Intelligence Organization Act of 1979 provides that

> 17. (2) It is not a function of the Organization to carry out or enforce measures for security within an authority of the Commonwealth.

Similarly, the New Zealand Intelligence Organization Act 1969 provides that

> 4. (2) It shall not be a function of the Security Intelligence Service to enforce measures for security.

A similar provision should be included in the legislation governing Canada's security intelligence organization.

WE RECOMMEND THAT the legislation governing the security intelligence agency include a clause which expressly denies the agency any authority to carry out measures to enforce security.

(33)

A. POLICE POWERS

4. Under the present structure, those members of the Security Service who are regular members of the R.C.M.P. have the powers of peace officers as provided for in section 17(3) of the R.C.M.P. Act. These powers include the powers of arrest and of search and seizure conferred on peace officers by the Criminal Code of Canada, and additional powers conferred by other federal and provincial statutes. In our interviews with members of the Security Service we found that they rarely used their peace officer powers. Nonetheless, the possession of peace officer powers has continued, rather illogically, to be a requirement for management positions in the operational branches of the Security Service, thus posing a barrier to the civilian member's advancement.

5. There is no need for peace officer powers in a security intelligence organization which has as its essential function to collect, analyze and report intelligence. On the contrary, in terms of retaining checks and balances in the system, there is real advantage in not bestowing peace officer powers on its members. That is one reason why, in the previous chapter, we recommended that when members of the security intelligence organization exercise investigative powers involving the surreptitious entry of private premises or removal of private property, they should always be accompanied by a policeman who would deal with any breaches of the peace which may occur if the operation were to be suddenly interrupted. The definition of 'peace officer' in the Criminal Code is very wide and besides mayors, reeves, sheriffs, justices of the peace, wardens, prison guards, police officers, constables and bailiffs includes "... other person employed for the preservation and maintenance of the public peace...".[1] To remove any doubts, the statute governing the security intelligence organization should explicitly state that members of the organization are not to be considered peace officers.

WE RECOMMEND THAT members of the security intelligence agency should not have peace officer powers and that, to remove any doubt, the legislation establishing the organization should explicitly state that members of the security intelligence organization are not to be considered as peace officers.

(34)

B. PERMISSIBLE AND IMPERMISSIBLE PREVENTIVE ACTIVITIES

6. In Part III, Chapter 7 and again at the beginning of this chapter we took the position that the essential function of the security intelligence agency

[1] Criminal Code of Canada, section 2.

should be to collect, analyze and report intelligence and that the agency's mandate should not include certain types of countering and should exclude any executive powers for enforcing security. Here we will survey the various preventive or countering activities in which the R.C.M.P. Security Service has participated in the past and which might conceivably be envisaged for a security intelligence agency in the future, in order to set out more precisely which of these activities are permissible, which are dubious, and which are unacceptable. The principle of the rule of law which must apply to all security intelligence practices and policies requires a clear prohibition of any preventive or countering technique which violates any law — federal, provincial or municipal. The preventive techniques discussed below all relate to practices which are lawful.

Reporting security intelligence to governments and police forces

7. In the preceding chapter we reviewed the reporting functions of the security intelligence agency, pointing out the contexts in which components of the federal government and the R.C.M.P. require security intelligence in order to fulfill their responsibilities. In the next two chapters we shall consider the conditions under which the security intelligence agency should be authorized to transmit information to foreign governments and to provincial and municipal authorities in Canada. Such properly authorized transmission of security intelligence is not only a permissible way for the security agency to participate in preventing or countering threats to security but is indeed the overriding *raison d'être* for the existence of a security intelligence organization. But this reporting role, it must be emphasized, involves the transmission of information to public bodies — to police and government departments — under properly authorized law enforcement or security programmes.

Preventive security interviews or briefings

8. There are a number of contexts in which the security intelligence agency may wish to warn individuals and organizations in the private sector about threats to security. Canadian public servants or employees of private firms which have access to classified information who are about to be posted to missions in certain foreign countries, or civilians who are intending to travel in those countries, should be warned about the methods known to have been used by foreign intelligence agencies to compromise persons and through blackmail induce them to become sources for the foreign agency. We think this is an acceptable use of security intelligence and it is best for a member of the agency to give the briefing. However, such briefings should be given only to persons who are in a position to do serious damage to national security if they are compromised. Also, the agency should not use these briefings as a pretext for recruiting an individual to serve on a continuing basis as an intelligence source. In Chapter 4 of this Part we specified the conditions under which such continuing casual sources should be used as a means of collecting information. When those conditions are met and the agency is authorized to use a person who may travel abroad as a continuing source of information, it should not approach the individual in a surreptitious manner for that purpose. Openness

and voluntariness should be characteristics of the agency's security briefings of individual Canadians.

9. In the past, the Security Service has been known to communicate information to the employer of a person suspected of participating in, or supporting, a subversive activity, in order to jeopardize the employment of such persons (Vol. 41, p. 6709; Vol. 52, pp. 8426-7). We think that this practice is unacceptable. Denying a person employment in the public or private sector for national security reasons is a significant executive act which should be carried out only through authorized security clearance programmes. If the security intelligence agency has information indicating that a person in a firm which is carrying out defence-related work or work relating to national security is a security risk, it should pass that information to the department of the federal or provincial government responsible for the defence or security programme.

10. In at least one major Canadian city the Security Service undertook a programme of visiting senior officials in different sectors of community activity. One purpose of this programme was to make private employers aware of the availability of the Security Service in case they had reason to be concerned about subversive employees. We consider this a dangerous and unwise programme in that it is likely to lead to an exchange of information between private employers and the security intelligence agency which, again, may jeopardize the employment opportunities of individuals. Further, we do not think a security intelligence agency should advertise its services to the private sector. If the government deems it necessary to alert private organizations to the availability of the security intelligence agency to receive reports about threats to security, the government should do so through a vehicle other than the security intelligence agency.

11. We also think that the practice of giving security briefings to private groups to alert them to threats to security should not be permitted. Participation in activity of this kind may be perceived to be, or may in fact become, a propaganda campaign by the security intelligence agency. We think the dissemination of information about threats to security should be left to responsible Ministers. Mr. Justice Hope reached a similar conclusion with respect to the Australian Security Intelligence Organization:

> 248. It is no part of ASIO's intelligence dissemination function to publicize threats to security. Any D.G. of Security who reads s.5(1)(a) of the ASIO Act as authority to engage in propaganda, however 'laudable', embarks on a misconceived enterprise. The likely result is to bring discredit to ASIO.
>
> 249. A propaganda activity of this kind crosses the boundary between provision of information, which is proper, and the taking of a 'measure for security', which is not proper.
>
> 250. If warnings about the internal security situation are to be given publicity — whether attributably or not — that is something for the Government. It can seek advice from ASIO, or be offered it, and publish it. But the agency of publication should not be ASIO. Our system of government requires ministers to submit themselves to questioning in or out of Parliament. They have the responsibility and not ASIO.

> 253. If ASIO becomes involved directly in the public dissemination of security intelligence, it is likely to be accused of taking a partisan political position. It is most important that ASIO be above reproach in that regard. In many respects, its effectiveness depends on it having the confidence of all the major political parties.[2]

We agree with Mr. Justice Hope's reasoning. We would add that if the Director General or any other member of the security intelligence organization is to make a speech or otherwise appear in public to describe the work of the security agency or to give advice about threats to security, he must do so only with the permission of the Minister responsible for the agency, and only for the purpose of explaining or expounding government policy. In our view, for the reasons advanced by Mr. Justice Hope, the Minister would be well advised not to involve the Director General or other members of the agency in this kind of activity.

Relations with the press

12. For a number of years the Security Service carried on a press liaison programme, one purpose of which was to cultivate relationships with journalists that would enable the Security Service to "plant" certain material in the press. The articles were aimed at drawing attention to the security implications of certain events or the background or activities of certain individuals. (See, for example, Vol. 315, pp. 301427-63.) The cultivation of journalists was also designed to improve the Security Service's public image and to counter adverse publicity.

13. We think that the carrying out of a press liaison programme of this kind is seriously wrong. As we have said, it should not be a function of the security intelligence agency to publicize threats to security. If the agency requires any public defence of its activities or improvement of its image, this should be done by responsible Ministers. Secret intelligence agencies pose a serious threat to the democratic order when they endeavour to develop their own undercover media networks. That is why in our discussion of the use of human sources we recommended that the use of journalists as informants be very strictly controlled. We see no reason whatsoever for the security intelligence agency to maintain a press liaison programme or even a press liaison officer. Questions about the activities of the security intelligence agency should be answered by the Solicitor General or the Prime Minister. In Part VIII of this Report, we shall stress that one of the responsibilities of the Solicitor General, as the Minister responsible for the agency, is to provide opportunities for Members of Parliament and for the general public to study policy issues relating to the work of the security intelligence agency. It is important to provide a basis for a better public understanding of the function of the security intelligence agency, but this basis must not be established through a network of press relations established by the agency.

---

[2] Australia, *Fourth Report of the Royal Commission on Intelligence and Security*, Volume 1, pp.128-130.

Disinformation and smear campaigns

14. Attempts by a security intelligence agency to disrupt a domestic political group by circulating information about certain of its members constitute another category of unacceptable preventive activity. Such tactics, or "dirty tricks", are unacceptable even if they involve no breach of the civil or criminal law. The security intelligence agency should not be permitted to inflict damage on individual Canadians or Canadian organizations. In our liberal democratic system the state should administer sanctions against a citizen only when it has been established by due process of law that the citizen has broken the law. 'Disinformation' campaigns by the security organization run the risk of misleading not only the targetted group, but also other police forces and the government.

15. The prohibition of this type of disruptive activity should extend to the use of such tactics as anonymous letters or telephone calls designed to breed distrust amongst members or between factions of domestic political groups. It should not be a function of a security intelligence agency to break up Canadian political organizations, even those suspected of supporting or participating in activities constituting threats to the security of Canada, by trying to manipulate their affairs secretly. The collection of intelligence about such groups by the agency may well enable those who are responsible for law enforcement or other executive programmes to take action against such groups. The process of collecting intelligence, especially through informants and defectors from such groups, may well have disrupting effects. But spreading information deliberately in order to disrupt such groups should not be permitted.

Disruptive measures which mislead other government officials

16. In one case which was part of Operation Checkmate, Security Service officials did not raise security objections about a certain individual who was applying for Canadian citizenship. They reasoned that doubts might be raised among this person's colleagues, should he suddenly be granted citizenship after a number of prior refusals. There is no evidence to suggest that the Security Service officials informed either their own Minister, the Minister responsible for the Citizenship programme or the Interdepartmental Committee on Citizenship, the body of officials responsible for reviewing citizenship applications, about this operation.

17. It is our opinion that deceiving other government officials in this matter is unacceptable behaviour on the part of a security intelligence agency. Should the agency in future wish to use another government programme to help deceive one of the agency's subjects of surveillance, then the Minister responsible for the agency should inform the Minister responsible for the government programme in question and seek his concurrence or seek to have the other department take the required action.

Disruptive effects of double agents and informants

18. The use of informants by the security intelligence agency is very likely to have direct disruptive effects on penetrated groups or organizations. In the

counter-espionage field this is certainly the case with double agent operations, where an attempt is made to recruit a member of a hostile foreign service to be a source of information about the intentions and resources of the foreign agency and to influence the decisions of the foreign agency in a direction Canada would prefer.[3] Such operations, if successful, may enable the security agency to inflict serious damage on the foreign agency. The application of such methods in the counter-intelligence field against agencies of hostile foreign powers is an acceptable, indeed a highly desirable, preventive activity for the security intelligence agency, providing it is carried out in Canada. Similarly, the agency should be authorized and prepared to assist members of hostile foreign agencies who wish to defect while in Canada.

19. Informants may also be used by the security intelligence agency to gather information about a domestic political organization where there is reason to believe it is planning serious political violence. The presence of informants in such organizations may certainly have disruptive effects, but so long as the informant's primary purpose is to provide the security intelligence organization with information this is an acceptable activity. It becomes unacceptable when it is primarily a scheme of political interference designed to break up the organization. A cynic might say that in practice this will become a meaningless distinction: in our view it is a distinction which can be maintained, provided the members of the security intelligence agency understand and accept the reason for it. On the other hand, it will not likely be maintained if members of the agency, especially its senior officers, fail to appreciate that active intervention in the political process by a secret state agency endangers Canadian democracy.

20. Having said that an informant must not be injected into a domestic political organization for the primary purpose of disrupting the organization, even though it is planning political violence *generally*, we think that an informant who has penetrated a political organization for intelligence gathering purposes should be instructed that, when persons in the organization form an intent to commit a *specific* crime, the informant should try to discourage and inhibit the members of the organization from carrying out that crime. We note that such an instruction is included in the guidelines governing the F.B.I. use of informants, issued by the Attorney General, Mr. Levi, in 1976.[4] But we also note that in his testimony to a Congressional Committee, Mr. Levi stated that such disruptive actions must be "the minimum necessary to obstruct the force and violence" and "designed and conducted so as not to limit the full exercise of rights protected by the Constitution and laws of the United States."[5]

---

[3] For a good account of this counter-intelligence strategy in wartime, see John Masterman, *The Double Cross System*, New York, Avon Books, 1972.

[4] Attorney General's Guidelines for F.B.I. Use of Informants in Domestic Security, Organized Crime, and other Criminal Investigations, December 15, 1976. Quoted in John T. Elliff, *The Reform of FBI Intelligence Operations*, Princeton, New Jersey, Princeton University Press, 1979, Appendix IV.

[5] Quoted in John T. Elliff, *The Reform of FBI Intelligence Operations*, Princeton, New Jersey, Princeton University Press, 1979, p. 129.

21. In using the words "to discourage and inhibit" we wish to make it clear that in no way do we understand them to mean that the informant is licensed to break the law in order to achieve his specific objective of discouraging or inhibiting the crime. We envisage that there are ways of discouraging or inhibiting the commission of a specific crime which do not in any way entail the transgression of the law. To that extent we are in agreement with the Guidelines issued by Mr. Levi in 1976. Section 27 of the Criminal Code is a clear illustration of the latitude which may be exercised under the law. That section reads:

> Everyone is justified in using as much force as is reasonably necessary
>
> (a) to prevent the commission of an offence
>
> (i) for which, if it were committed, the person who committed it might be arrested without warrant, and
>
> (ii) that would be likely to cause immediate and serious injury to the person or property of anyone or
>
> (b) to prevent anything being done that, on reasonable and probable grounds he believes would, if it were done, be an offence mentioned in paragraph (a).

Defusing

22. 'Defusing' is a technique designed to reduce the possibility of violence by groups. It is accomplished by having members of the security intelligence agency speak to members of the group, letting it be known that the agency is aware of the group's plans to use violence. The expectation is that this will cause the group to have second thoughts. Also the agency might point out acceptable non-violent ways in which the group can pursue its political objectives. Such defusing programmes or 'constructive encounters' have been said to be analogous to the English policeman's gentle and good natured admonition to members of a restless crowd to "move along, there". We consider that a word of caution and encouragement to use non-violent means of publicizing a group's cause are perfectly proper techniques of preventing disorder in a democratic society. However, we are not convinced that such defusing actions should be a responsibility of Canada's security intelligence agency.

23. Under the statutory mandate which we have recommended for the agency, much of what might be referred to as civil disorder would not be within the purview of the security intelligence agency. The resort to violence by political groups should be of interest to the security intelligence agency only when it constitutes terrorism or a serious threat to the democratic order. But even where the threat of political violence is within the intelligence collection mandate of the agency, we do not think it is the most appropriate body to attempt defusing actions. It would be preferable for police forces, with local peace officer responsibilities, to employ such techniques. There is also a practical consideration: using members of the agency in such a programme decreases their availability for covert operations by revealing their identity as members of the agency to too many people.

Conspicuous surveillance

24. 'Conspicuous surveillance' is a technique of intimidation whereby members of a security intelligence agency, by making a group aware of their presence, attempt to frighten the group into abandoning its meeting or demonstration. To equate such conspicuous surveillance by members of a security intelligence agency with the presence of uniformed police officers at a public meeting or demonstration at which violence may break out is to use a false analogy: the presence of policemen in those circumstances is a legitimate means of dampening the possibility of immediate violence. They are identifiable as police and there is nothing in their deployment that smacks of intimidation by the state for a purpose other than law enforcement. It is not acceptable to use security intelligence officers in civilian clothes, in large or small numbers, to intimidate Canadians attending political meetings, even meetings at which the intention to use political violence is promulgated.

25. The common theme in our approach to the techniques of countering or preventing threats to security is that the security intelligence agency should not be permitted to carry out activities or disruptive measures designed to inflict damage on Canadian citizens or domestic political groups. The agency should concentrate on the collection and analysis of intelligence, the 'countering' of foreign intelligence agency operations in Canada, and the transmittal of intelligence to the appropriate departments of government so that *they* may take whatever action *they* deem to be in the public interest. A distinction should be drawn between the extent to which 'countermeasures' are taken against spies and international terrorists on the one hand, and against domestic subversive groups on the other. In the former cases, it is permissible to 'weaken' the adversary by recruiting an agent in place who will attempt to shape the decisions of the hostile agency or group, or by encouraging a hostile agent to defect. But in purely domestic matters, the purpose of penetration should be solely the collection of intelligence rather than disruption. Of course, if the target is a Canadian citizen acting as a foreign agent these activities are not a purely domestic matter, but even in this case we consider it undesirable for the agency to engage in any disruptive activity if the Canadian is an active member of a recognized Canadian political party. In domestic matters, if there is evidence of the commission of a crime, the security intelligence agency may turn it over to the police having jurisdiction in criminal matters, a perfectly acceptable kind of countering in all situations.

26. We do not recommend any system of prior approval of countering measures, because we do not envisage the use of any countering measures which are not part of authorized and acceptable intelligence collection methods. Some might regard the position we have taken against countering programmes by a security intelligence agency as unreasonably severe. However, we believe that this position is justified on the basis of the damage which the employment of such techniques, even when lawful, may do to the democratic process and to the security intelligence agency itself. Nothing has done more to discredit secret intelligence agencies in the western democracies, including Canada, than their perpetration of 'dirty tricks' on the citizens of their own country. The securing of democracy requires an effective security intelligence

agency. That effectiveness requires that the agency have broad public support. That support must not be alienated by unacceptable countering or disruptive activities.

WE RECOMMEND THAT the security intelligence agency not engage in making known to employers in the private sector its availability to receive information about employees alleged to be subversives, and that any such advice as to such availability should, if the government considers such advice to be desirable, be transmitted through another department or agency.

(35)

WE RECOMMEND THAT it not be a function of the security intelligence agency to publicize, outside government, threats to the security of Canada; and accordingly, the security intelligence agency should not maintain liaison with the news media; and further, that all public disclosure about the activities of the security intelligence agency should be made by responsible Ministers.

(36)

WE RECOMMEND THAT the security intelligence agency not be permitted to disseminate information or misinformation in order to disrupt or otherwise inflict damage on Canadian citizens or domestic political organizations.

(37)

WE RECOMMEND THAT if the security intelligence agency wishes to use another government programme to help deceive one of the agency's subjects of surveillance, the Solicitor General should seek the concurrence of the Minister responsible for the programme in question.

(38)

WE RECOMMEND THAT the security intelligence agency not be permitted to use informants against domestic political organizations primarily for the purpose of disrupting such organizations.

(39)

WE RECOMMEND THAT an informant of the security intelligence agency who has penetrated a political organization for intelligence gathering purposes should be instructed that, when persons in the organization have formed an intent to commit a *specific* crime, the informant should try to discourage and inhibit the members of the organization from carrying out that crime, but that the informant must not transgress the law in order to discourage or inhibit the commission of the crime.

(40)

WE RECOMMEND THAT it not be a function of the security intelligence agency to carry out defusing programmes and that the agency not be permitted to use conspicuous surveillance groups for the purpose of intimidating political groups.

(41)

C. INTERROGATION OF SUSPECTS

27. In Part III, Chapter 10, we pointed out that there may be interrogations of persons within the Security Service suspected of having become agents for a

foreign intelligence agency. Here we wish to stress the importance of observing the law in conducting such interrogations. So long as the Security Service is within the R.C.M.P., the provisions of the R.C.M.P. Act and Regulations as to the questioning of regular members must be adhered to. Civilian members are not subject to the same rules. If a civilian member is suspected, he must not be detained for questioning unless the police are prepared to arrest him for an offence. Of course, if a civilian member does not co-operate willingly, he will certainly prejudice his employment.

28. If a member of the security intelligence agency or an employee of another federal government department is questioned (for example an employee of the Department of External Affairs who has returned from a foreign posting) the members of the security intelligence agency must remember that there is in our law no general power to detain for questioning.[6]

29. If, as we recommend, the functions of the Security Service are in the future exercised by a security intelligence agency separate from the R.C.M.P. and without police powers, it will be particularly important to ensure that the members of the agency are conscious that, just as the police have no power to detain anyone against his will for questioning, so too no civilian person has such a power.

[6] Leigh, *Police Powers in England and Wales*, London, Butterworth's, 1974, p. 29.

CHAPTER 7

INTERNATIONAL DIMENSIONS

INTRODUCTION

1. The origins of many of the threats to Canada's internal security are located outside of Canada. Clearly, the security intelligence agency whose function it is to provide advance intelligence about threats to Canada's security should be able to obtain information about the foreign sources of these threats.

2. There is a considerable body of public information about international trends and events which the security intelligence agency can and should use. For instance, the branch that deals with Communist bloc intelligence activities and the branch that deals with Marxist and Leninist organizations in Canada should have a capacity for analyzing publications describing the international policies of Communist countries and international trends in Marxist and Leninist political movements. The security intelligence agency should also have effective liaison with the Department of External Affairs so that it can make good use of the understanding of international trends acquired by Canadian missions abroad.

3. However, because of the highly secretive character of foreign security and intelligence agencies and international terrorism, much information about activities directed against Canada's security from abroad cannot be obtained through public sources of information. Canada, unlike most of its allies, has not developed a foreign intelligence service. When we speak of a foreign intelligence service we mean an agency which collects abroad, by overt and covert means, intelligence on security, economic, political and military matters relating to other countries, which may be of interest to Canada. On occasion, and more in the distant past than in recent years, Canada has used secret agents abroad to collect information pertinent to Canada's internal security. But for the most part Canada has relied on its allies for foreign intelligence about threats to the country's security.

4. There is some information that friendly foreign agencies will not collect, if only because they have no need to or no interest in doing so if their national interests would not be served. Some of this information may be obtained through extensions abroad of security intelligence investigations initiated in Canada. In this way an extra-territorial dimension is added to the activities of the Canadian Security Service. In section A of this chapter, we explore the circumstances in which we think it appropriate for members or agents of the security intelligence agency to go abroad for operational purposes.

5. Information provided by the intelligence agencies of a large number of countries has been an important source of security intelligence for Canada in the past. It has not been forthcoming without a willingness on the part of Canada's Security Service to exchange information. In section B of this chapter, we will look at some of the current problems involved in the exchange of information with foreign agencies. We will suggest that guidelines be drawn up to govern such relationships generally, and that terms of reference governing particular relationships with foreign agencies conform to these guidelines. We also suggest the kinds of information which should and should not be exchanged, and outline a system of controls for monitoring relationships.

6. In section C we turn to a more speculative question: whether or not Canada should establish its own secret foreign intelligence agency. We make no recommendations on this subject, but urge that it be carefully studied. To look at this question following our consideration of the foreign activities of the Canadian security intelligence agency and its relations with foreign agencies is, we think, appropriate, since part of the difficulty in defining the proper circumstances for members of the security intelligence agency to go abroad arises from Canada's lack of a foreign intelligence service. As regards relations with foreign agencies, this country is in a position of considerable dependence on its allies for information necessary for the identification of security threats to Canada.

A. FOREIGN OPERATIONS UNDERTAKEN BY THE SECURITY INTELLIGENCE AGENCY

7. What, if any, operations should the security intelligence agency conduct outside Canada? Currently this issue, as it affects the R.C.M.P. Security Service, is clouded by a lack of clear guidelines within that agency, together with a lack of clear policy within government. This is compounded by confusion as to what constitutes 'defensive' and 'offensive' activities. Consideration of overseas operations carried out by the security intelligence agency is made more difficult, in the Canadian context, by the fact that Canada does not deploy a foreign intelligence service engaging in espionage in and against foreign countries. The difficulty arises from the resulting notion that the Canadian Security Service has not operated secretly abroad. It has, from time to time. While Canadians have not conducted espionage abroad, they have collected information secretly. This has created sensitivity both inside and outside government concerning Canadian security intelligence activities carried out in foreign countries.

8. Questions concerning a security intelligence agency's operations abroad are closely related to questions concerning the agency's relationships with "friendly" foreign agencies. If Canada wishes to obtain intelligence about activities in other countries which threaten the security of Canada, intelligence not openly available, Canada must either collect the information covertly or obtain it from an intelligence agency of a friendly country. To the extent that Canada chooses not to collect such information itself it must depend on obtaining this informa-

tion from friendly agencies. We will examine these arrangements in section B of this chapter.

Historical background

9. The historical section of our Report (Part II, Chapter 2) showed that there was a time in Canadian history when security intelligence was collected on a systematic basis, at least in the United States. This was particularly true of the period between 1864 and 1871 when Sir John A. Macdonald personally directed Gilbert McMicken's Western Constabulary to infiltrate Fenian groups in the United States. Thereafter, foreign intelligence operations became more spasmodic. At the turn of the century, rumours of American plots to annex the Yukon were investigated through the surveillance of suspected plotters in the United States and Canada, and through the infiltration of some American miners' organizations. The first World War saw further activities in the United States, directed principally from British Columbia, against agents suspected of espionage and subversion. The information from these operations was sent to Ottawa and to British authorities. Before the United States' entry into World War I the Commissioner of the R.N.W.M.P. directed, from the Force's Headquarters in Regina, investigations of persons of German and Austrian extraction suspected of launching espionage or sabotage activities against Canada from the western United States.

10. Since the formation of the R.C.M.P. in 1920, there has been no systematic collection overseas of security intelligence information by the Force. We have no evidence that this practice arose from a decision of government. Apparently it was a decision reached within the R.C.M.P. The policy did not, in itself, imply there was no need for Canada to collect information overseas. It simply meant that Canadians would not be deployed abroad to collect secretly such information.

The proper scope of security intelligence activities outside Canada

11. In the past, policy discussions of the Security Service's foreign operations have frequently focussed on the distinction between an 'offensive' and a 'defensive' intelligence agency. It has been argued that, because the Security Service is strictly a 'defensive' service, it should not operate abroad. According to this argument foreign operations should only be carried out by an 'offensive' agency. We do not find this distinction between an 'offensive' and 'defensive' agency helpful, since the distinction could refer to three different aspects of intelligence operations:

(i) the kind of intelligence which an agency seeks

(ii) whether the collecting agency attacks foreign agencies which are targetted against Canada or waits to defend itself against foreign attacks

(iii) the geographic location of the agency's activities.

Discussions of 'offensive' and 'defensive' intelligence agencies often fail to make clear which of these three aspects is being referred to. Failure to

distinguish amongst them may lead to great confusion in defining the proper scope of the foreign operations of a security intelligence agency.

12. First, so far as the nature of intelligence being sought is concerned, the mandate we have recommended for the security intelligence agency might be termed 'defensive' in the sense that the intelligence it seeks must pertain to threats to Canadian security. Its intelligence mandate should be confined to activities against the security of Canada generated by others — individuals, groups or countries. In this sense the security intelligence agency is a *counter-intelligence agency*, not an espionage agency.

13. Turning to the second dimension of a security intelligence agency — whether it attacks or simply defends — it is also clear from what we have recommended with regard to the use of countering activities (e.g. double agent operations in the counter-espionage field) that the security intelligence agency should not be entirely confined to a defensive posture. In Canada, but not abroad, it should be able to attack foreign agencies by penetrating them and gaining defectors; it should not be required to wait until it, or some other branch of Canadian government, is being attacked. To borrow from the language of sports, the best defence is sometimes a good offence.

14. Now, turning to the third dimension — the geographic location of the security intelligence agency's activities — we do not think that the agency should be required to confine its intelligence collecting or countering activities to Canadian soil. If security intelligence investigations which begin in Canada must cease at the Canadian border, information and sources of information important to Canadian security will be lost. Thus a total ban on security intelligence operations outside Canada would be an unreasonable constraint. If to operate abroad is 'offensive', then Canada's security intelligence agency should be offensive in this sense, although we are cognizant of the very great risks — diplomatic, moral and practical — in carrying out security intelligence activities abroad. Because of these risks it is important to confine such activities to those that are essential, to subject them to a clear and effective system of control, and to ensure that they are always within the mandate of the security intelligence agency. In what follows we shall endeavour to define more precisely the circumstances in which a security intelligence agency should be permitted to extend its operations abroad and the controls which should apply to such operations.

Current practice

15. Covert Security Service operations outside Canada today are conducted on an *ad hoc* basis. These cases involving foreign travel always arise from an internal security investigation begun in Canada. Generally, the rationale for such operations is that the information sought relates directly to the internal security of Canada and is not the kind of information that can be or should be obtained through liaison with friendly security and intelligence agencies.

16. It is important that the distinction be made between occasional travel abroad by members of the R.C.M.P. Security Service for operational purposes, and the activities of R.C.M.P. liaison officers posted to Canadian missions

abroad. The 48 liaison officers stationed in 26 posts abroad perform two functions for the Security Service: they screen immigrants applying for entry to Canada in order to establish which individuals have criminal records or are suspect from a security point of view, and they carry out liaison with the police and security agencies of the host country. The liaison officer's functions do not include the direction of cases involving the collection of intelligence by covert means.

17. Many nations deploy both a security intelligence agency and a foreign intelligence service. Canada is unique among its close allies in that it does not have a secret foreign intelligence service. This country's non-involvement in covert foreign operations, or espionage, was most recently stated by Prime Minister Trudeau, when he told the House of Commons that:

> We have never, to my knowledge, certainly not under my government, engaged in any espionage abroad in the sense that we have not been looking for information in an undercover way in any other country.[1]

18. To clarify the circumstances under which foreign operations might be permitted, we felt it might be helpful to review past operations. The cases we reviewed could be divided into three categories which correspond to low, medium, and high levels of risk in foreign operations: the element of risk pertains not only to the individuals concerned, but to Canada's relations with the state against whom the operation is mounted, or the state in which it takes place. In the course of this work we identified some areas where a high risk was evident. If Canada is to mount foreign operations in the future, it is our view that it is inappropriate for a Canadian security intelligence agency to carry out some particular types of high risk operations.

19. Decisions as to when a foreign operation by the security agency should be permitted must be guided by a balancing of costs and benefits. Without attempting to be exhaustive, we would suggest that at least the following considerations be taken into account:

(a) the intelligence 'target' of the foreign operation must be one which is within the security intelligence agency's mandate;

(b) a foreign operation involving clandestine activity should be undertaken only for the purpose of obtaining information which is of great importance to the security of Canada, or for maintaining an intelligence asset which is of great importance to the security of Canada;

(c) wherever possible the security intelligence agency should work co-operatively with the security agency of the host country; the cumulative effect of unilateral Canadian operations abroad might invite retaliatory actions which could be detrimental to Canada's security and foreign relations;

(d) transgressions of foreign laws would not be taken as having been authorized by the mere fact of authorization having been granted for travel to a foreign country, and the agency should place the problem before the Cabinet for a decision as to what should be permitted;

---

[1] House of Commons, *Debates*, January 10, 1974, p. 9227.

(e) the Minister responsible for the security intelligence agency and the Minister of External Affairs should be kept adequately informed of security intelligence operations outside of Canada.

We turn now to the controls which should regulate foreign operations of a security intelligence agency.

Controls

20. Under the present system there are certain stages through which a foreign operation must go for approval before the operation occurs. We examined these stages, and it is significant that within these reporting relationships, as now prescribed, there is no provision for notifying the Solicitor General, the Minister responsible for the Security Service.

21. So far as control within the security intelligence agency is concerned, we think the Director General should be notified of all foreign operations. As the chief executive officer of the security intelligence agency, he should have the opportunity to question any foreign operations and to veto those which he thinks are inadvisable. There may be emergency circumstances in which the Director General is not immediately available, in which case he should name his deputy on a *pro tem* basis, as responsible for giving his approval for any such operation.

22. At the ministerial level we think that it is intolerable to continue with a situation in which the Minister responsible for the security intelligence agency is not informed of foreign operations. The Director General should notify the Solicitor General before initiating any foreign activity involving a member of the agency or its informants. The Minister's review of such proposals should be based on a set of policy guidelines, prescribed by him, governing foreign operations. These guidelines would incorporate the factors suggested in paragraph 24 above. These guidelines should also be approved by the Cabinet Committee on Security and Intelligence and disclosed to the special Parliamentary Committee on Security and Intelligence. It is important that guidelines in this area be subject to a collegial interdepartmental approval process, as they should reflect the various concerns of government that must be balanced in determining the advisability of foreign operations by an intelligence agency. The statute governing the activities of the agency should include authorization to operate abroad.

23. We recognize the need to ensure that foreign operations by a security intelligence agency are co-ordinated with the requirements of Canada's foreign relations. Even though we anticipate that the number of foreign operations undertaken by the security intelligence agency will be low, still certain of these operations might, if improperly handled, cause grave damage to Canada's international relations or run counter to Canada's foreign policy objectives. We do not think, however, that all foreign operations by a security intelligence agency incur such risks. Some of the cases we reviewed involve low-level risks. Moreover, in our view, it would be desirable that in any foreign operations contemplated in the future, the following two practices be followed:

(1) The Minister responsible for the security intelligence agency should notify the Department of External Affairs in advance of any operations entailing significant risks to Canada's foreign relations. In an emergency situation, a foreign operation could go ahead with the provision that notification took place *ex post facto.*

(2) On an annual basis, the Director General and appropriate officials of the security intelligence agency should meet with the Under Secretary of State for External Affairs and the Deputy Under Secretary of State for Security and Intelligence to review foreign operations completed, currently being undertaken, or proposed by the security intelligence agency.

The system we propose recognizes that it is a ministerial responsibility to ensure that the Department of External Affairs is consulted in advance about foreign operations with serious implications for foreign policy and provides a process whereby the Department of External Affairs can be kept comprehensively informed of the security intelligence agency's foreign operations.

24. There may well be situations in which the Department of External Affairs would consider that the risk to Canada's foreign relations exceeds the potential worth of the security intelligence that might be obtained from a foreign operation. In resolving differences of this kind it is important that one set of interests should not automatically take precedence. Thus, when the Solicitor General and the Secretary of State for External Affairs could not agree over a foreign operation, the matter should be decided by the Prime Minister.

WE RECOMMEND THAT for intelligence purposes falling within the security intelligence agency's statutory mandate and subject to guidelines approved by the Cabinet Committee on Security and Intelligence, the security intelligence agency be permitted to carry out certain investigative activities abroad.

(42)

WE RECOMMEND THAT the Director General of the security intelligence agency inform the Minister responsible for the agency in advance of all foreign operations planned by the security intelligence agency.

(43)

WE RECOMMEND THAT in cases which on the basis of policy guidelines are deemed to involve a significant risk to Canada's foreign relations, the Minister responsible for the security intelligence agency inform the Department of External Affairs sufficiently in advance of the operation to ensure that consultation may take place.

(44)

WE RECOMMEND THAT the Director General and appropriate officials of the security intelligence agency should meet with the Under Secretary of State for External Affairs and the responsible Deputy Under Secretary on an annual basis to review foreign operations currently being undertaken or proposed by the security intelligence agency.

(45)

B. RELATIONSHIPS WITH FOREIGN AGENCIES

25. One of Canada's major sources of intelligence about security threats to this country comes from foreign security and intelligence agencies. The largest suppliers of such information are agencies of countries with which Canada is closely allied. Even if this country had its own secret intelligence service working abroad, there would still be a need for agreements with foreign agencies.

26. Relationships with foreign security and intelligence agencies inevitably involve a sharing or exchange of intelligence: in order to receive information, Canada must be willing to give information to those agencies. The notion of reciprocity is, then, central to successful liaison relationships with foreign agencies.

27. Liaison with foreign agencies raises a number of important policy concerns. One is, simply, whether true reciprocity exists. There is always a danger that, unless the exchange of information is carefully monitored, Canada may give far more than it gets. A second concern relates to the entering into agreements which may conflict with Canada's foreign policies. An agreement should not be made with the agency of a foreign country if it would entail implicitly condoning policies which Canada has opposed as a matter of our foreign policy. A third issue involves the need for sufficient control over information leaving this country to ensure that the rights of Canadians are adequately protected.

28. These and other issues all point to the need for careful and accountable control by government of liaison agreements between the Canadian security intelligence agency and foreign agencies. From our review of this subject, it is evident that there has been a lack of government attention to the policy issues inherent in such agreements, a neglect which can create an excessive vulnerability to the hazards of liaison with foreign agencies.

29. Another, less tangible, problem related to foreign agreements is the danger of Canada's security intelligence agency adopting the outlook and opinions of a foreign agency, especially of an agency which has come to be depended upon heavily. This danger is particularly acute because Canada does not have its own foreign intelligence agency, so that a Canadian Security Service may become extremely dependent on foreign agencies for covert information. This tendency to adopt the views and analyses of a foreign agency would be offset if the security intelligence agency had at its disposal expertise capable of providing analyses derived from open literature. The R.C.M.P. Security Service has had few members capable of providing analyses of foreign situations with possible effects on Canadian security.

30. Some central issues have to be addressed regarding the identity and nature of the partners with whom the government is willing to enter into relationships, the extent of agreements including the kinds of information to be exchanged, and the procedures to be established to ensure that the agreements or relationships reflect both the wishes and the needs of the Canadian

government while balancing security interests with foreign policy interests. In what follows, we will set out our recommendations on these matters.

Agreements with foreign agencies

31. Relationships with foreign agencies are covered by a variety of agreements, both formal and informal, enduring and occasional, covering the exchange of different kinds of information and services. The R.C.M.P. currently has relationships with foreign agencies providing for many types of exchange, including information regarding terrorism, visa vetting of immigrants, information given to foreign agencies on Canadian emigrants, and information regarding counter-espionage. This list is not exhaustive, but it gives some idea of the variety of relationships entered into by the R.C.M.P. Security Service.

32. One characteristic of the development of these relationships has been their *ad hoc* nature. They have been entered into as a result of a perceived need within the R.C.M.P. and have not been subject to an over-arching set of government guidelines. A more fundamental objection to the development of these previous agreements is that the Solicitor General, the Minister responsible for the R.C.M.P., has not been adequately informed about them until very recently. In 1977, the then Solicitor General, Mr. Fox, asked the R.C.M.P. to provide him with a list of all existing foreign liaison arrangements. To attempt to comply with the wishes of the Minister, the Security Service had to solicit information from its operational branches: no central record existed. It was only after much research by us and by the R.C.M.P. that by 1980 it had been determined that there were, in fact, arrangements with a great many countries. We mention this to emphasize the absence of any recording or control of such an important network of arrangements. As a result, the R.C.M.P. has proceeded independently to develop foreign agency arrangements in an area of foreign policy concern.

33. This is not to suggest that relationships with foreign agencies have been of a *sub rosa* nature. We simply make the point that two obvious points of control, the Department of the Solicitor General and the Department of External Affairs, have remained largely in ignorance of the existence or terms of such relationships. While we appreciate the sensitivity of information exchanges and the consequent need to limit knowledge of their existence within the government, we feel it particularly unsatisfactory that the Solicitor General, the Minister responsible for the Security Service, has not been consulted, nor his agreement sought, in the establishment of relationships with foreign security and intelligence agencies.

34. We think that the statutory mandate of the security intelligence agency should explicitly provide that there may be foreign liaison agreements subject to proper control. The principal points of control should be the two Ministers, the Solicitor General and the Secretary of State for External Affairs. No agreement should be entered into without terms of reference approved by the two Ministers. The terms of reference for each agreement with a foreign agency should specify what types of information or service could be exchanged

(for example, immigration visa vetting, and intelligence on terrorists). These terms of reference, while recorded within the Canadian government, need not necessarily be written down or formally agreed upon with the foreign agency. Some foreign agencies would withhold their cooperation if the Canadian security intelligence agency insisted on formal written agreements.

35. If agreement on terms of reference cannot be reached between the Secretary of State for External Affairs and the Solicitor General, the decision would be made by the Prime Minister. We would anticipate that any such disagreement would arise from competing considerations relating to foreign policy and security. It is important that one Minister not have the power of veto over a particular set of terms of reference, and that disagreements be resolved by the Prime Minister or the Cabinet.

WE RECOMMEND THAT the statutory mandate of the security intelligence agency provide for foreign liaison relationships subject to proper control.

(46)

WE RECOMMEND THAT the terms of reference for each relationship specify the types of information or service to be exchanged.

(47)

WE RECOMMEND THAT the terms of reference for each relationship be approved by the Solicitor General and the Secretary of State for External Affairs before coming into effect and that any disagreement be resolved by the Prime Minister or the Cabinet.

(48)

36. The government should establish a clear statement of principles to guide the security intelligence agency's relationships with foreign security and intelligence agencies. One purpose of these guidelines would be to diminish the risk of the security agency's becoming an appendage of foreign agencies, particularly in relation to those agencies from whom it borrows information frequently. These principles should be developed as a set of guidelines by an interdepartmental committee, and approved by Cabinet. In the following paragraphs, we suggest some of the principles that should be reflected in these guidelines.

Exchanges of information with foreign agencies

37. As we have indicated, an effective Canadian security intelligence agency requires information and intelligence from foreign agencies to meet Canadian needs. These foreign agencies may provide not only useful general assessments of potentially or actually dangerous situations, but also intelligence concerning individuals who may come to Canada or who are already here. Given the reciprocal nature of these relationships, the Canadian security agency must be willing to provide similar kinds of information in return.

38. With this understood, we are of the opinion that certain precautions have to be taken with regard to the information provided to foreign agencies by the Canadian security intelligence agency. In 1971, for example, Assistant Commissioner Parent sent letters to four foreign agencies enclosing the R.C.M.P.'s brief on the Extra-Parliamentary Opposition (E.P.O.) which included the

names of individuals in the Canadian Public Service believed to be involved to a greater or lesser degree in that movement, and the names of some individuals who were not even suspected of involvement. We have no objection to the provision of the general assessment of the situation to other agencies. Rather, our objections to this action are twofold: first, the evidence on which the E.P.O. list of names was based was not reliable and was therefore potentially misleading to a foreign agency as well as harmful to individual Canadians; and second, there was no knowledge of the use, if any, to which the information was to be put by the foreign agencies, nor any procedure for recovering the information once it had been used. There appears to have been, and there still appears to be, no consciousness on the part of the R.C.M.P. of these concerns in respect of that information. That, if symptomatic of a general attitude, is most disheartening and alarming.

39. The principle of reciprocity may also induce the Canadian security authorities, in their position of dependence, to enter into relationships with foreign agencies without giving adequate weight to possible conflicting foreign policy considerations. A lack of sensitivity in this area will, almost inevitably, create friction with those responsible for directing Canada's external relations.

40. A third facet of reciprocity is the assessment of the flow of information in and out of Canada. A relationship with a foreign agency which consistently results in a net outflow of information is clearly one which should be examined for its usefulness to this country. This is not to suggest that the R.C.M.P. Security Service's participation in the world intelligence community is not valued by its allies. It is important to Canada in terms of, for example, terrorism and foreign intelligence activities. Moreover, if Canada were unwilling to collect information and to exchange it with foreign agencies, there is the danger that those agencies would take steps to get it themselves in Canada, by developing agents and sources in this country. These real or potential problems, together with lesser ones not set out here would, we feel, be overcome by the precepts which follow.

41. There should be records of the transmittal by the security intelligence agency to foreign agencies of information concerning Canadian citizens, or persons in Canada, or Canadian organizations.

42. As well as recording the transmittal of information, the so-called 'third party rule' must apply to such information in order that some semblance of control be retained over Canadian proprietary rights to the information, although it is recognized that such 'control' may well be somewhat illusory. The third party rule stipulates that information given by one agency to another may not be passed on to a third agency or party without the approval of the original agency. This rule should govern further use of the information by the recipient, and would also facilitate its retrieval. The difficulty of retaining any real control over information sent to another agency is illustrated by the inability of the R.C.M.P. to recover information it had supplied for more than twenty years to a foreign agency. In June 1978, pursuant to a decision previously taken by Mr. Fox, Mr. Blais instructed the R.C.M.P. to cease providing such information and requested the return of information previously

provided. At the time of writing this Report the requested information has not been returned.

43. The information given to foreign agencies must be about activities which are within the statutory mandate of the Canadian security intelligence agency. Foreign agencies are likely to have different mandates and therefore are likely to ask for information about Canadians or about people in Canada which is beyond the Canadian agency's terms of reference. When this occurs, the Canadian security intelligency agency must refuse to go outside its mandate, even though this may result in a reciprocal loss of information for Canada. In Chapter 5 of this part of the Report, we set out our views on what information received from a foreign agency should be reported by the security intelligence agency. We said that, with few exceptions, the agency should report only information relevant to threats to the security of Canada as defined in its mandate.

44. We take the view, too, that the Canadian security intelligence agency, as a pre-condition for passing information to a foreign agency, should know the reason for the request. To provide information without questioning the request invites the danger that the security agency will operate according to the mandate of a foreign agency rather than according to its own terms of reference.

45. Management of liaison arrangements must take into account the importance to Canadian security of maintaining a relationship between the Canadian security agency and its foreign counterpart. In relationships where Canada is the net beneficiary in the flow of information, this will be a particularly important consideration. In exchanges involving information on international terrorism or counter-intelligence, there will likely be little conflict of interest. A more probable source of difficulty would seem to us to be in exchanges of information on domestic subversion, where Canada's standards may differ from those of the foreign agency seeking information, and where there may be insufficient concern for the protection of the interests of Canadian citizens.

46. Moreover in our opinion, it should be a fundamental principle that information disclosed by a potential immigrant within the immigration process is for the sole and exclusive use of the Canadian government, and should not be further disseminated or disclosed, unless there is a clear and important reason related to Canada's security and the approval of the Director General of the Canadian security intelligence agency has been obtained.

The exchange of services and joint operations

47. Cooperation with a foreign agency may also entail some joint operations with that agency. The cooperation may take the form of lending a human source to the foreign agency, borrowing a source from the foreign agency, or providing or receiving some other support. An instance in which the R.C.M.P. Security Service borrowed from a foreign agency was that of Warren Hart. The Security Service of the R.C.M.P. has also undertaken joint operations with friendly foreign agencies within Canada. We are satisfied that these operations have been approved by the Security Service as being justified in the Canadian

interest, and that every reasonable effort has been made to ensure that friendly foreign agencies not conduct operations on Canadian territory without the prior approval of the Security Service. As mentioned earlier, however, we are not satisfied with the extent to which the Minister has been informed of the occurrence of such operations.

48. We believe that all cases involving the exchange of sources must have the approval of the Director General of the security intelligence agency. Such cases must be within the mandate of that agency, hence relevant to Canadian security, and should, in addition, be carefully controlled by Canada. In cases where a foreign security agency requests assistance which falls outside the mandate of the Canadian security agency but concerns a criminal matter, the request should be passed on by the security intelligence agency to the relevant police force in Canada. In this way, the security agency would act as a central clearing house and recorder of requests from foreign intelligence agencies. Such a procedure would permit an effective review of such operations by the independent review body.

49. Elsewhere, we have reported on the use by the R.C.M.P. Security Service of journalists in the writing and publication of articles containing information believed by the Service to be true. If such a practice were to involve the R.C.M.P. in attempting to arrange Canadian publication of foreign information, that would be both dangerous and undesirable, because it could result in information being published in Canada which is both unreliable and inconsistent with Canadian interests. Toleration of such a practice would open the door to the possibility of foreign manipulation of Canadian public or official opinion. That would be unacceptable. As stated earlier in this Report, any publication of material at the instigation of the Security Service should require the approval of the Director General of the security agency and his Minister. This would apply both to articles of foreign origin and to those inspired by press contacts within the agency.

50. A final aspect of the exchange of services between foreign agencies and the Canadian security intelligence agency concerns security screening for immigration purposes on behalf of a foreign agency. Under our recommendations for screening in Part VII of this Report, the security intelligence agency would carry out few field investigations. It should have a tightly circumscribed mandate to collect information about character reliability for Canadian purposes and should not collect this information on behalf of a foreign agency. Foreign agencies must not be allowed to carry out their own field checks here. They must rely on interviewing individuals in their own country or at their consulate or embassy in Canada. In sum, only limited aid could be given to a foreign agency in this area, and that assistance would have to coincide with the Canadian screening programme. Any assistance beyond this would have to be negotiated on a government-to- government basis.

Obtaining security intelligence outside liaison arrangements

51. It may be necessary for the Canadian security intelligence agency to obtain information otherwise than through a liaison arrangement, from a foreign country whose law forbids the dissemination of information to foreign

governments. As we will point out in Part VII, Chapter 2, to authorize the Canadian security intelligence agency to establish a paid source, or otherwise to break the laws of a foreign country in order to obtain information about one of its citizens, would be imprudent. To us, a more attractive alternative would be bilateral discussions between the two governments to obtain the information. In most cases, interviews with potential immigrants will suffice.

52. The normal exchange of security intelligence may, with some countries, be prevented by a lack of cooperation between the Canadian security agency and the host agency. One solution is to rely on the assistance of the agencies of friendly countries who have members there, and who may be able to advise the Canadian authorities of security information relevant to a potential immigrant. This procedure carries with it some risk of exposure and subsequent embarrassment to the Canadian government. In such cases, risks must be weighed against potential benefits and the decision incorporated into the terms of reference drawn up for the relationship with the friendly agency.

Statement of principles

53. The foregoing discussion indicates a number of the principles which should be incorporated into guidelines governing the security intelligence agency's relationships with foreign agencies. Briefly, we would suggest that these guidelines include the following principles:

(a) all relationships should have approved terms of reference;

(b) all transmittal of information by the security agency should be recorded;

(c) the third party rule should operate so that the information transmitted to a foreign agency may be retrieved when it is no longer needed;

(d) the security agency should be aware of the reason for the request from the foreign agency and that reason must relate in some way to the security of the requesting country;

(e) all exchanges must be within the mandate of the security intelligence agency and hence relate to the security interests of Canada;

(f) Canada must control all foreign agency operations in Canada;

(g) the Director General of the security agency must approve of each joint operation; and

(h) the Minister responsible for the agency should be notified when a member of the agency goes abroad on behalf of the agency.

WE RECOMMEND THAT the Government establish a clear set of policy principles to guide the security intelligence agency's relationships with foreign security and intelligence agencies and that the Joint Parliamentary Committee on Security and Intelligence be informed of these principles.

(49)

WE RECOMMEND THAT the information given to foreign agencies by the security intelligence agency must be about activities which are within the latter's statutory mandate; that the information given must be centrally

recorded; that the security intelligence agency know the reasons for the request; and that the information be retrievable.

(50)

WE RECOMMEND THAT the Director General approve of each joint operation with a foreign agency and ensure that Canada control all foreign agency operations in this country.

(51)

WE RECOMMEND THAT the Solicitor General be informed of each joint operation, or operation of a foreign agency, in Canada.

(52)

Liaison officers abroad

54. The recommendations for change which we have presented here should not, in any substantial way, alter the current arrangements pertaining to R.C.M.P. liaison officers. Currently, all such liaison officers come under the R.C.M.P.'s Director of Foreign Services which is not part of the Security Service. We anticipate that, even with a separate security intelligence agency, it should be possible to substitute a member of that agency for a member of the R.C.M.P. in those posts that, at present, have more than one liaison officer. In those missions where now there is only one liaison officer from the R.C.M.P., it should be possible for a single liaison officer to supply information to both the R.C.M.P. and the security agency. As both organizations, under our proposals, would report to the same Minister, he should ensure that the liaison function involves no unnecessary duplication of services and that there is effective cooperation between the R.C.M.P. and the security agency.

55. The recruitment and training programme outlined elsewhere in this Report would, we feel, better prepare individuals for international postings. These individuals should have diplomatic status as has recently become the case with some R.C.M.P. liaison officers.

56. The relationship between the liaison officer and the Head of Post should remain as at present and as laid down within the terms of reference formulated for the Foreign Service of the R.C.M.P. These state that liaison officers will serve as an integral part of the mission, and will be responsible to the Head of Post. Despite the clear need for communication between these two individuals, we take the view that if the liaison officer wishes specially to safeguard some security intelligence by sending it to his headquarters without clearing it with the Head of Post, he should be able to do so. The receipt of such information should be recorded by the security agency headquarters so that, except in extraordinary circumstances, the Under-Secretary of State for External Affairs has access to it. Where extraordinary circumstances exist, the Director General should disclose them to the Solicitor General. The decision to widen access to this information would then rest with the appropriate Ministers and not with their representatives at a foreign mission.

57. The post-war period has seen western missions in the U.S.S.R. and eastern Europe under persistent and increasingly sophisticated technical surveillance by Soviet and Soviet bloc intelligence agencies. Throughout this period, a great deal of evidence has been collected by western security and

intelligence agencies about the use of microphones, radio transmitters, and other forms of eavesdropping and electronic interception equipment used against their missions. It is very often unknown what time lag there has been between the installation and its discovery. It has been, and continues to be a most serious problem. Historically, there has been disagreement within some departments and agencies of government as to the extent of the threat and, therefore, the resources that should be available to counter it. The departments and agencies of government should, through suitable intragovernmental arrangements, arrive at agreement on this type of threat and on the resources necessary to meet it.

WE RECOMMEND THAT the security intelligence agency have liaison officers posted abroad at Canadian missions to perform security liaison functions now performed by R.C.M.P. liaison officers, except that in missions where the volume of police and security liaison work can be carried out by one person, either an R.C.M.P. or a security intelligence liaison officer carry out both kinds of liaison work.

(53)

WE RECOMMEND THAT the relationship between the liaison officer representing the security intelligence agency and the Head of Post be governed by the terms of reference as laid down for the Foreign Services of the R.C.M.P., but that the security intelligence agency's liaison officer have the right to communicate directly with his Headquarters and independently of the Head of Post when the intelligence to be transmitted is of great sensitivity. Except in extraordinary circumstances, which should in each case be reported by the Director General to the Solicitor General, such communications should be made available to the Under-Secretary of State for External Affairs.

(54)

WE RECOMMEND THAT the government examine, on a regular basis, both the resources which are being devoted to the technical security of Canadian missions abroad, and the policies and procedures which are being applied to the security of those missions.

(55).

Review of foreign liaison activities

58. In addition to ministerial responsibility, we advocate three other points of reference for these activities. First, the security intelligence agency's annual report to Cabinet should include an account of the agency's foreign liaison activities. Second, the independent review body should ensure that the agency's relationships with foreign agencies fall within the statutory mandate and meet the guidelines set out by government. This review would be facilitated by the central recording of the terms of reference governing particular relationships. Third, the Joint Parliamentary Committee on Security and Intelligence should be informed of the principles governing such relationships and, where possible, should have access to the terms of reference of particular relationships. If a foreign agency objected to the terms of its relationship with Canada's security intelligence agency being disclosed to members of the Committee, then the Canadian government would have the choice of foregoing that relationship or of refusing the Committee's access to the terms of the relationship.

WE RECOMMEND THAT the security intelligence agency's relationships with foreign agencies be subject to the following forms of review:

(a) An account of significant changes in these relationships be included in the security agency's annual report to the Cabinet;

(b) relations with foreign agencies be subject to continuing review by the independent review body;

(c) the Joint Parliamentary Committee on Security and Intelligence be informed of the principles governing the security agency's relations with foreign agencies and, to the extent possible, of the terms of reference of particular relationships.

(56)

C. SHOULD CANADA HAVE A FOREIGN INTELLIGENCE SERVICE?

59. Canada is unique among its major allies in not deploying a foreign intelligence service. While we are in no position to carry out a comprehensive review of Canada's foreign intelligence needs, a general look at the question of a secret foreign intelligence service is a natural outgrowth of our consideration of the policies and procedures governing a security intelligence service. We have already shown how the lack of a foreign intelligence agency limits the effectiveness of a security intelligence organization. In the previous section, we showed how Canada, through liaison arrangements with 'friendly' intelligence agencies, compensates, to some extent, for the lack of a foreign secret service of its own. Also we think it important to consider how the system of government control and accountability which we are recommending for a security intelligence agency should apply to a foreign intelligence service, if and when Canada decides to establish such a service.

Previous studies of Canada's foreign intelligence needs

60. There would have been little need for us to comment on this subject if previous studies of Canada's intelligence needs had examined the subject comprehensively, but those to which we have had access make virtually no mention of it.

61. The more recent general reviews of which we are aware are four in number.

62. Perhaps the most important of these studies was one carried out in 1970. Significantly, many of the points made regarding the lack of integration of intelligence with governmental decision-making are still valid one decade later. It noted the emphasis on military intelligence in Canada and the need for this country to follow the Americans and the British in a greater use of political and economic intelligence. The government was advised of the need for greater co-ordination of intelligence at the centre, via the intelligence committees, and to some extent this advice has been taken. A more general aim of the study, like others later, was to question, first, if Canada was getting its money's worth from certain areas of its intelligence program and secondly, if the collected intelligence was being used as efficiently as possible.

63. The various studies came to the conclusion that Canada was indeed getting its money's worth from its multilateral intelligence arrangements and allowed that the arrangements were, in fact, a bargain. The second question as to whether or not the best use was made of the intelligence, was directly or inferentially answered in the negative. The further study, carried out on economic intelligence, was set up specifically to look at the linkages between producers and consumers and methods of improving the use made of this intelligence within the consuming departments.

64. All of these studies pointed to two further, and potentially serious, shortcomings. The first was that the mechanisms for determining Canada's foreign intelligence priorities and requirements were inadequate. The second shortcoming was the lack of intelligence analysis either within departments or on an interdepartmental basis. Despite widespread agreement that the analytical capacity should be strengthened within the intelligence community, little would appear to have been done to bring it about.

65. The first shortcoming, the lack of definition of priorities and requirements, has to some extent been offset, at least so far as foreign intelligence is concerned, by the establishment of suitable intragovernmental arrangements. It should be remembered, however, that a definition of requirements and priorities depends in some measure on an analysis of current intelligence holdings and on identification of areas or subjects that require further intelligence collection. In short, an inadequate analytical capability will contribute to a lack of clarity in the definition of requirements and priorities. Where there is a need for detailed information, such as in tactical or current intelligence on particular issues, this vagueness in definition will impede the collection process. In matters of broad strategic intelligence, the lack of precision in defining requirements and priorities will be much less of an impediment to effective direction of the collectors.

66. Although the weakness of the intelligence analysis function was recognized in the past, it has not been remedied to date. A proposal we shall develop later in this Report, that the Intelligence Advisory Committee have a responsibility for writing current intelligence assessments and that a Bureau of Assessments be established to provide strategic assessments, would, we believe, be the basis for overcoming this shortcoming in Canada's intelligence system.

The external environment and changing intelligence needs

67. A nation's intelligence requirements depend on a variety of factors, such as its political, economic, and military aspirations, its geographic location, and its involvement in regional organizations. Meeting these requirements does not necessarily involve covert information only; in fact, most of the collection effort, at least in human terms, will probably be focussed on gathering overt information. The extent to which a nation collects covert foreign intelligence through its own resources will depend, among other things, on its financial resources, its ethics, its international posture and the extent to which it believes it can rely on its allies.

68. There has been a paucity of analysis of non-military intelligence requirements in Canada. The current multilateral arrangements were formulated and continue to function largely within the context of East-West relations and the military blocs which underpin those relations. These arrangements for sharing intelligence have been based on mutual aims and a common perception of threats. Political intelligence which is processed information on other nation's international political relations does not, generally, have this element of commonality; it entails a national, rather than collective, need. Similarly, economic intelligence, despite the interdependence of the leading economic powers, tends to be more national and less multinational in perspective. The emergence of non-military concerns as dominant foreign policy issues of western nations has altered intelligence requirements. The emergence of energy, for example, as a pre-eminent foreign policy issue, reduces the commonality of interests between advanced western nations.

69. This skewing of national intelligence needs, away from military intelligence and towards greater emphasis on economic intelligence, places Canada in a situation which is quite different from its earlier post-war experience. One result of the emergence of new issues and the changes in the international climate in the past decade, has been the blurring of the once clear distinction between one's friends and those whose friendship is less manifest or reliable. While these changes have not, from a military point of view, altered the alignment of forces and so given rise to novel military intelligence requirements, there is a demonstrably greater need for political and economic intelligence for national purposes.

Factors to be considered in deciding whether Canada should establish a foreign intelligence service

70. A first step in considering those intelligence requirements which are related to Canada's distinctive national interests is to identify those national needs that cannot be met through liaison arrangements with allies. There is likely to be a quite narrow set of intelligence requirements, of a political or economic nature, or related to Canada's domestic security, which is either of no interest or of a competitive rather than a collaborative interest to Canada's allies. However few in number, such requirements should be identified. The second step is to determine how the intelligence needed in these areas can be collected, if it is not available from overt sources. There are, generally, two means of collecting intelligence covertly. The first is technical collection. The second method is through human sources conducting espionage.

71. Human sources have the great advantage of being able to yield intelligence about human intentions — and it is frequently knowledge of intentions which is most valuable in defending a country's political and economic interests as well as warning it of foreign threats to its internal security. Another advantage is cost: human sources cost much less than technical sources, all the more so if only a small organization is envisaged with a capacity for collecting intelligence in only a limited number of places. While we are not in a position to put a price on establishing a secret intelligence service — the costs of its

equipment, training facilities, and professional support services, for example, we understand that the cost of operating a small service is modest.

72. The costs of *not* having a capacity for collecting foreign intelligence relevant to distinctive Canadian interests must be considered. The experience of some foreign countries suggests that the intelligence product of a modest secret service has been useful to these nations. How much more security and intelligence information would Canada receive from its allies if it contributed more to the common pool? While this cannot be answered firmly, it is not unreasonable to suppose that the amount of intelligence available to Canada would increase. Foreign experience indicates that information is available to a country's foreign intelligence agency through liaison with other agencies that does not flow either to its diplomats or to its domestic security service.

73. While it is possible to outline some of the benefits which might accrue to Canada by establishing a limited secret intelligence service, there are also some readily identifiable liabilities. To begin with, there is a clear political risk in a government directing espionage activities against other states. The image of honesty and straightforwardness in the conduct of international affairs may produce benefits to this country, particularly within a Commonwealth setting, that cannot be readily measured. What potential penalties might be incurred in acknowledging the existence of a Canadian secret intelligence service? The issue seems to centre on the notion of 'image'. That image, however, is somewhat misleading, given our use of intelligence obtained by the espionage services of other countries.

74. It is difficult to gauge the political costs incurred by democratic countries who do deploy secret services. Unquestionably, as the recent situation in Iran vividly demonstrates, the conduct of secret intelligence activities abroad can have dire effects on a country's international relations and the security of its citizens. Risks of this kind can be reduced but not eliminated by confining a foreign intelligence agency to the collection of intelligence and denying it any mandate for political intervention or para-military operations.

75. There is also a serious moral issue involved in a government employing a secret agency whose *modus operandi* requires it necessarily to break the laws of other nations. It may be argued that the existence of an agency with such a mandate brings with it a risk of influencing the practices of a country's security intelligence agency. Lawbreaking can become contagious both within a country's 'intelligence community' and amongst those senior officials of government and the national political leaders who are responsible for directing the intelligence community. Were this to happen in Canada it could seriously undermine reforms which we hope will be put in place to guard against illegality and impropriety in the activities of the security intelligence agency and the R.C.M.P. On the other hand, it may be argued that so long as this risk is recognized, and the proper controls are in effect, the risk of such influence and contagion can be minimized.

76. We do not know the extent to which Canada's abstaining from foreign espionage has been based on moral or political considerations. It may have been based more on a judgment that Canada's allies provide so much intelli-

gence to this country that our basic foreign intelligence requirements can be met from these sources. Whether or not this is a correct interpretation of past policy, we do not know. However, we do believe that a careful analysis of the various costs and benefits is overdue and that a review should be carried out so that Canada's policy on this particular feature of its intelligence capabilities might be decided upon in an informed and mature manner. In urging that there be further study of this matter we emphasize that we are referring only to the *collection of intelligence*; we are not in any way suggesting that the Canadian government should even examine whether or not it should have a service which may be used to destabilize foreign governments or attack their leaders.

Organizational and governmental aspects

77. While we make no recommendations either for or against the establishment of a secret foreign intelligence service, we do think it important to indicate how, organizationally and in terms of government direction, such a service should relate to a security intelligence agency.

78. In our view, it would be extremely important to keep such an agency separate from the security intelligence agency. We have already mentioned the dangers of contagion with respect to an espionage agency's practice of violating the laws of other countries. Further, it is clear to us that the intelligence which such an agency collects would go well beyond the purposes of security intelligence. It would be unwise to combine very different intelligence collection responsibilities within a single agency. In addition, there is a danger of creating a security and intelligence monolith in a democratic state. Demarcation lines between the two services, dealing with the foreign and domestic overlap of the two, would have to be carefully drawn.[2]

79. If a foreign intelligence agency were to be established by Canada it should not be done in the surreptitious fashion in which such agencies have been established in other countries. In the western democracies we have surely learned by now the need to subject intelligence agencies to the basic precepts of democratic and responsible government. This means at the very least that a Canadian foreign intelligence agency should have a clear charter approved by Parliament. While working out a legislative mandate is not without difficulty, the task should be easier than recent American experience indicates, for in that country the biggest difficulties have centered on notification of Congressional Committees, and approval of covert operations involving political interference in the affairs of foreign countries, rather than on intelligence collection. As a Canadian service should not have a mandate to indulge in active measures of intervention, drawing up a charter to cover the collection of secret intelligence might be somewhat less complicated and controversial. In addition to a prohibition on active measures, we would not envisage a secret service having any paramilitary functions.

[2] See, for example, John Bruce Lockhart, "Secret Services and Democracy", *Brassey Annual Review*, 1975-76; and "The Relationship Between Secret Services and Government in a Modern State", *Journal of the Royal United Services Institute for Defence Studies*, June 1974.

80. A legislative mandate should also specify the controls to which such a service would be subjected and also provide for Executive and Parliamentary review of its activities.

81. Finally, it is almost axiomatic that the government should develop an assessment capacity not solely within the collecting agency. Recent experiences abroad amply illustrate the dangers of maintaining the two functions wholly within one agency. Thus the establishment of a strengthened capacity at the centre of government for assessing intelligence and defining intelligence priorities along the lines proposed in Part VIII of this Report would be an essential prerequisite for an expanded foreign intelligence collection capability.

CHAPTER 8

RELATIONSHIPS WITH OTHER DEPARTMENTS PROVINCIAL AND MUNICIPAL AUTHORITIES

INTRODUCTION

1. In this chapter, we examine the relationship of the security intelligence agency with other governmental bodies having security and intelligence responsibilities. The chapter has two sections. In the first, we focus on what some refer to as the federal government's 'security community'. We concentrate most of our attention on two departments — the Department of External Affairs and the Department of National Defence. Other departments are also affected by our recommendations but in this chapter we indicate only the general nature of these changes and where they are dealt with in this Report. In the second section of this chapter, we explain the relationships between the security intelligence agency and provincial and municipal authorities. Our general theme throughout both parts of this chapter is the need for a higher degree of co-operation among those government bodies whose activities in some way affect the security of Canada.

A. RELATIONSHIPS WITH OTHER FEDERAL GOVERNMENT DEPARTMENTS AND AGENCIES

2. In earlier chapters of this Report, we noted that the R.C.M.P. has made formalized written agreements with a significant number of federal government departments and agencies. Many of these agreements have sections relating to the Security Service. We have expressed our concern, particularly in several chapters in Part III, with the contents of some of these agreements. Here, we wish to register our deep concern over the fact that most of these agreements were not submitted for approval by the Solicitor General, the Minister responsible for the R.C.M.P. These agreements do not deal with trivial matters; many have an important bearing on significant policy issues affecting R.C.M.P. operations. Moreover, as we pointed out earlier, some of these agreements are questionable on grounds of legality and propriety. We believe that the Deputy Solicitor General and the Director General of the security intelligence agency should ensure that all agreements which are made between the agency and other federal government bodies and have significant implications for the conduct of security intelligence activities be brought to the

attention of the Solicitor General for his approval. The Solicitor General should inform his colleagues on the Cabinet Committee on Security and Intelligence of the nature of these agreements.

3. The unwillingness on the part of the R.C.M.P. to seek the Solicitor General's approval of agreements with other departments is another manifestation of one of the Force's principal weaknesses: its poor capacity for dealing effectively with other departments and agencies of government. Nowhere is this weakness more apparent than in the Security Service's relationship with the Department of External Affairs.

The Department of External Affairs

4. As we have stated throughout this Report, many of the threats to Canada's security emanate from abroad. This single fact demands the closest of co-operation between the Department of External Affairs and the security intelligence agency. Until recently, however, they have not enjoyed a close relationship. In some ways, the tension and suspicion between the two bodies is almost inevitable: the Department of External Affairs is committed to an easing of international tensions based on co-operation and understanding; the Security Service tends to view the activities of many foreign countries with deep suspicion. The result is a difference of views on the threats to this country's security which originate abroad. One example of how these differing points of view lead to conflict is in deciding the appropriate course of action in the case of a foreign diplomat engaging in improper intelligence activities. While the Security Service has generally favoured the prompt expulsion of these diplomats, the Department of External Affairs, either through fear that Canadian diplomats will be expelled in reprisal or because of the timing of a certain diplomatic initiative, has not always agreed to declare these diplomats *personae non gratae*. Such differences, we should note, are not peculiar to Canada. In the nations with which we are most familiar, similar tensions exist between those organizations charged with the conduct of foreign relations and those concerned with the conduct of security and intelligence activities. The situation in this country, however, is worse than it needs to be, in part because of the wide differences in educational background and work experiences of the staff of the two organizations. We think that some of our recommendations will help this situation, principally those dealing with the recruitment and training of personnel for the security intelligence agency. Such measures will go some way towards encouraging a greater measure of sophistication in the analysis of international affairs by the agency, a change that in itself we would hope will reduce the current disparities in the views of the Department of External Affairs and the Security Service.

5. While mutually negative attitudes have been part of the underlying tension between the two bodies, an attempt has been made by both of them since the mid-1970s to provide mechanisms for improving the process of co-operation.

6. We believe that a Memorandum of Understanding is one means of ensuring compatibility between Canada's security intelligence activities — which have international effects — and its foreign policy endeavours. Conse-

quently we recommend that the separate and civilian security intelligence agency, the creation of which we propose in Part VI, draw up a memorandum of understanding between itself and the Department of External Affairs. This document should be prepared by the respective deputy ministers, the Under Secretary of State for External Affairs and the Deputy Solicitor General, and submitted for approval to their Ministers. It should cover the appropriate aspects of security and intelligence co-operation and co-ordination listed above. We now consider the general principles which should be contained in this memorandum. The changes we are recommending call for a higher degree of involvement by the Secretary of State for External Affairs and his officials in setting security intelligence policy and in deciding on specific operations with international implications.

(i) *Consultation*

7. There are at present regular meetings between the Deputy Under Secretary of State for External Affairs (Security and Intelligence) and the Director General of the Security Service. We think it would be desirable to continue this practice after the formation of a separate and civilian security intelligence agency. In addition, there is a need for the Deputy Solicitor General and the Under Secretary of State for External Affairs to discuss on a regular basis important questions of policy requiring resolution. The role of the Deputy Solicitor General in these policy discussions is consistent with the recommendations we make in Part VIII, Chapter 1, calling for this official to be more active in directing and controlling the security intelligence agency.

(ii) *Foreign operations undertaken by the security intelligence agency*

8. In the previous chapter, we set out the need for a set of guidelines for foreign operations of the security intelligence agency. Further we recommended that the Cabinet Committee on Security and Intelligence, of which the Secretary of State for External Affairs is a member, should approve such guidelines. Under our recommendations, the Solicitor General and his deputy have the main responsibility for ensuring that the guidelines are adhered to by the security intelligence agency. Our recommendations also call for periodic reviews of the guidelines by officials in the Department of External Affairs and the security intelligence agency in the light of past operations. The security intelligence agency should consult with the Department of External Affairs in advance only concerning those foreign operations with significant implications for Canada's foreign relations.

(iii) *Counter-intelligence operations in Canada*

9. Counter-intelligence operations in Canada are of concern to the Department of External Affairs when they involve foreign nationals working in this country, or diplomats working out of their missions here who are suspected of intelligence activities. In Chapter 4 of this part of the Report, we discussed information collection methods to be employed by the security intelligence agency. We recommended the establishment of three basic levels of investigation. The third level, what we have called the full investigation, requires a

three-stage initiating procedure. It is at the first stage, in which senior officers of the security intelligence agency and officials of government departments consider the merits of proposals for full investigation, that we think the Department of External Affairs should be consulted in certain circumstances when proposals have a bearing on foreign relations. We should emphasize that External Affairs should not have a power of veto over security operations. (Differences between the security intelligence agency and External Affairs which cannot be resolved at the official level must be taken up at the ministerial level.) Nevertheless, our recommendations here call for a higher degree of involvement of the External Affairs Minister and his officials in important operational decisions.

(iv) *Agreements between the security intelligence agency and foreign agencies*

10. Our principal recommendation here, as set out in Part V, Chapter 7, was that future agreements conform to guidelines to be formulated by the Cabinet Committee on Security and Intelligence and approved by Cabinet.

The Department of National Defence

11. The Department of National Defence has responsibilities to provide "aid of the civil power" under section 233 of the National Defence Act.[1] Under this section, the Chief of the Defence Staff must comply with a request for troops from a provincial attorney general in

> ... any case in which a riot or disturbance of the peace requiring such services occurs, or is, in the opinion of an attorney general, considered as likely to occur, and that is beyond the powers of the civil authority to suppress, prevent or deal with.

The Chief of the Defence Staff has the authority, however, to determine what resources are required to deal with a particular situation. (We discuss "aid of the civil power" in more detail in Part IX, Chapter 1.) To help the Department of National Defence perform these responsibilities, there are arrangements for the exchange of intelligence and information concerning the threat to internal security. It is recognized that the flow of information is primarily one way — from the Security Service to the Department of National Defence.

12. Under the mandate we are proposing for Canada's security intelligence agency, there will continue to be a need for close co-operation between the Department of National Defence and the new agency. The Department has other needs for security intelligence information in addition to "aid of the civil power". Securing Canadian Forces bases across the country and being aware of the activities of foreign spies interested in Canada's military secrets are two such examples. We consider it necessary, therefore, that the Deputy Solicitor General, the Deputy Minister of National Defence and the Chief of the Defence Staff negotiate a Memorandum of Understanding to be ratified by their respective Ministers.

[1] National Defence Act, R.S.C. 1970, ch.N-4.

13. Our recommendations in Part VII with respect to the security screening process will not significantly alter the Department of National Defence's security screening role in regard to its own employees. The Department would continue to call upon the R.C.M.P. for criminal records checks, and would request information from the security intelligence agency about activities which are threats to security as defined by Parliament. The Department could carry out field investigations, as it now does, provided that these investigations are confined to information about a person's character and personal qualifications and are consistent with the role we have recommended for security staffing officers from the Public Service Commission or government departments. (See Part VII, Chapter 1.)

14. As for communications security, the security intelligence agency would continue the Security Service's role of providing technical advice and intelligence about threats to security to all those in government responsible for maintaining communications security. The R.C.M.P.'s "P" Directorate would retain its lead role in establishing and monitoring the maintenance of standards in technical security matters such as in computer security. The Department of National Defence would thus liaise with both "P" Directorate and the security intelligence agency on these matters.

Other federal government departments and agencies

15. We refer the reader to the appropriate chapters of our Report where our recommendations have important implications for the relationship of the security intelligence agency to other federal government departments and agencies. There are four such chapters. Our recommendations for the security screening of the Public Service in Part VII, Chapter 1 have an important impact on other government departments and especially the Public Service Commission. Then, in Part VII, Chapter 2, where we discuss security screening for immigration purposes, we suggest a number of changes affecting the Canadian Employment and Immigration Commission. In Part VIII, Chapter 1, we examine the interdepartmental security and intelligence committee system, and here again, our recommendations have important implications for several government departments. Finally, in Part IX, Chapter 1 we discuss the subject of crisis management, another area of interdepartmental endeavour for the security intelligence agency. In all of these chapters, our aim is to ensure that the relationships of the agency with other government departments conform to the mandate we are recommending for the agency, help the agency become better integrated with the rest of government, and provide the agency with continuing 'feedback' about the usefulness of the information it is providing.

WE RECOMMEND THAT the Solicitor General approve all agreements which the security intelligence agency makes with other federal government departments and agencies and which have significant implications for the conduct of security intelligence activities.

(57)

WE RECOMMEND THAT the security intelligence agency, once it has separated from the R.C.M.P., negotiate a Memorandum of Understanding with the Department of External Affairs.

(58)

WE RECOMMEND THAT the Deputy Solicitor General, the Deputy Minister of National Defence and the Chief of the Defence Staff negotiate a memorandum of understanding to be ratified by their respective Ministers.

(59)

B. RELATIONSHIPS WITH PROVINCIAL AND MUNICIPAL AUTHORITIES

16. In a federal state, the relationship between federal security authorities and provincial governments and the police forces under their authority is extremely important. Australia and the Federal Republic of Germany are considerably ahead of Canada in establishing an effective system of liaison between the national security agency on the one hand and the governments and police forces of the member states on the other. Granted that each federal state must achieve inter-governmental co-operation according to its own constitutional traditions and institutional arrangements, still we think there is room for much improvement in federal, provincial and municipal liaison on national security matters in Canada. To a large extent we think that improvement in this area depends on recognition by the federal authorities that from a practical point of view Canada's security should not be treated as a water-tight compartment of exclusive federal responsibility and that effective protection against security threats requires the co-operation of provincial and municipal authorities. We develop this theme further in examining the following five areas: security screening, V.I.P. protection, liaison with provincial police and security organizations, co-operation between federal and provincial ministers, and the investigation of criminal activity by members or sources of the security intelligence agency.

Security screening

17. The provision of security screening services by the R.C.M.P. for provincial and municipal authorities has a long history. Here we summarize briefly only the highlights of this history. In 1954, R.C.M.P. Commissioner Nicholson agreed to undertake 'subversive' and criminal records checks for the police forces that were members of the Chief Constables' Association of Canada. The Ontario Provincial Police and the Metro Toronto Police were the only forces to take advantage of the offer. An R.C.M.P. policy was adopted in 1957, and reaffirmed in 1963, which approved assistance to contract provinces (those provinces that, under arrangements with the federal government, use the R.C.M.P. for policing, both on a provincial and municipal basis) under strict conditions, whereby the provincial attorney general could request background security checks on provincial government employees. An arrangement with a non-contract province occurred in October 1971, when the Quebec Police Force set up screening arrangements with the R.C.M.P. for the Centre d'Archives et Documentation (C.A.D.), a security intelligence advisory Committee for the Quebec government. Under this arrangement the Quebec Police Force did the field investigation and the R.C.M.P. did the criminal and subversive records checks. As requests grew dramatically, the Quebec govern-

ment under Premier Robert Bourassa adopted a screening document similar to the federal government's Cabinet Directive 35 (CD-35), the document setting out security criteria for employment in the federal Public Service. From 1971 to 1977, the Security Service conducted over 6,000 security screening checks on behalf of the Quebec authorities.

18. In June 1978, the R.C.M.P. Security Service in South Western Ontario submitted a memorandum seeking clarification of the federal government's policy in relation to the screening of applicants for the Ontario Provincial Police, and the Metro Toronto Police Department, and for sensitive positions within the Ontario government. This request led to a review of the screening service provided by the R.C.M.P. Security Service to police forces and provincial governments, and to an examination of the authorizations for providing this service. Because CD-35 did not specifically authorize screening services for agencies outside of the federal government, the Director General of the Security Service, Mr. Dare, gave instructions on June 29, 1978 to suspend this screening service.

19. While the programme was suspended pending the Solicitor General's decision, Mr. Dare, in a letter to Mr. Bourne, the Assistant Deputy Minister, Police and Security Branch, provided two reasons in support of continuing the vetting service. The first was that joint operations between federal, provincial and municipal security and police agencies required close co-operation. Hence, it would be desirable that municipal and provincial participants in these joint operations be security cleared. Second, the screening of some provincial and municipal government employees was defensible on grounds of national security. Employees with access to sensitive information involving, for example, the administration of justice, the vital points programme, or emergency measures, should be "loyal, reliable and of good character". Consequently, Mr. Dare proposed that the R.C.M.P. should respond to (a) requests from an attorney general which had a bearing on national security and (b) requests from a provincial or municipal law enforcement agency which was a member of the Canadian Association of Chiefs of Police. The Honourable Jean-Jacques Blais, the Solicitor General, gave his authorization for a resumption of the screening service on an interim basis. Before the service resumed, however, the government changed and the matter was not acted upon by the new Solicitor General, the Honourable Allan Lawrence. The present Solicitor General, the Honourable Robert Kaplan, has also not authorized the resumption of this service.

20. We believe that there are distinct advantages in the security intelligence agency providing security screening services to provincial governments and to provincial and municipal police forces. The provision of such services should improve communication between federal and provincial bodies with security responsibilities and may facilitate further federal-provincial co-operation. In addition, there is a real danger that security intelligence services, established in part to perform this service, will proliferate at the provincial level. Increasing the number of such services in Canada would appear to us to complicate the control and monitoring of security intelligence activities. In recommending that the federal government provide screening services upon request to provincial governments and provincial and municipal police forces, we emphasize that the

Solicitor General should approve all such requests for a screening programme and that the security intelligence agency should provide only information that is within its mandate to collect. Thus, those provincial and municipal bodies receiving the screening services should have primary responsibility for assessing character reliability. Finally, we believe that it would be highly desirable for a province using this screening service either to establish its own review mechanisms for persons who believe that they have been treated unfairly in the screening process, or to 'opt into' the federal review system which we propose in Part VII, Chapter 1.

21. What should happen if the security intelligence agency, in the course of an investigation not connected with a provincial screening programme, comes across information relating a provincial public servant or politician to a security threat? In our examination of Security Service files, we discovered that at least one such case had occurred within the last 10 years. A regionally based Security Service officer approached a provincial premier in order to warn him about the activities of certain members of his party. We believe that a security intelligence agency should report security relevant information to provincial politicians and officials, but the agency should exercise great care in doing so. Otherwise, as we noted in Part V, Chapter 3, it runs the risk of damaging the very democratic process which it has been established to secure. Given the sensitivity of such matters, we believe that the agency should seek the approval of the Solicitor General before reporting security relevant information relating to provincial politicians or public servants.

V.I.P. security

22. A further aspect of security work in which a high degree of federal-provincial co-operation is required is in the protection of V.I.P.s such as members of the Royal Family, the leaders of other countries and Canadian dignitaries. Currently, "P" Directorate of the R.C.M.P. is responsible to the federal government for protecting V.I.P.s, a responsibility that involves liaison with provincial authorities and also with the R.C.M.P. Security Service. The Security Service is expected to provide "P" Directorate with assessments regarding security threats to V.I.P.s including the potential for violence developing at international events taking place in this country. It is not the role of the Security Service to provide the actual protection, but rather the intelligence on which protective measures can be based. It falls to "P" Directorate to produce the actual plans and details of protection. In performing this function, "P" Directorate often must solicit the help of provincial and municipal police forces who will assist in the role of providing protection. In the past, disagreements have arisen either because, in "P" Directorate's view, too much security has been provided or, alternatively, too little has been provided.

23. We believe that a more systematic process of co-operation and co-ordination is necessary. In line with some foreign experience, we think that a formal mechanism should be established to co-ordinate V.I.P. security measures. To this end, it would be useful for the government to study the evolution and practice of the co-operative and co-ordinating machinery that exists in Australia and in the Federal Republic of Germany. The recently established

Australian machinery is particularly interesting. In proposing the establishment of a Standing Advisory Committee on Commonwealth-State Co-operation for Protection against Violence, the Australian Prime Minister stated that its purpose was to achieve "the highest degree of efficient operation and co-operation on a nationwide basis"[2] in providing advice to government about politically motivated violence. It meets every six months. In Canada, there now exists federal-provincial-municipal co-ordinating machinery for dealing with various kinds of crises. Similar machinery could be developed for V.I.P. security. One facet of this co-ordinating machinery might be written agreements between various levels of government. These should set out, we think, the duties of the law enforcement agencies and also the role of the security intelligence agency as the collector of intelligence and the body responsible for taking the lead role in assessing the degree of threat. In this way, and with a central body for co-ordination, the degree of overlap between the jurisdictions might be reduced and protective security measures more effectively co-ordinated between them.

Liaison with police and provincial security organizations

24. V.I.P. protection is only one among many security concerns requiring co-operation between the security intelligence agency and domestic police forces. With the creation of a separate and civilian agency at the federal level, liaison problems may increase at least in the short term, because of the traditional reluctance on the part of police forces to share criminal intelligence information with members of an agency who are not policemen. To help overcome these problems, we make two suggestions. First, the security intelligence agency should establish a special liaison unit, staffed in part by personnel with police backgrounds. The major responsibility of this unit would be to facilitate the exchange of security relevant information with domestic police forces and to encourage co-operation. Second, following the example of its Australian counterpart, the security intelligence agency should attempt to develop written agreements with major domestic police forces. These agreements, among other things, would establish liaison channels, specify the types of information to be exchanged, and indicate under what conditions joint operations could be conducted. The Solicitor General should approve such agreements.

25. The potential problems connected with joint operations deserve special comment. The evidence given before us of the joint operation against the A.P.L.Q. (Operation Bricole) by members of the Montreal City Police, the Quebec Police Force, and the R.C.M.P. Security Service illustrates that the planning for this operation took place at the local level in isolation from Security Service Headquarters. Because there was no plan approved by Headquarters, the respective roles of the three forces were unclear. The R.C.M.P. officer who was asked to approve the actual surreptitious entry of A.P.L.Q. offices was under the impression that the R.C.M.P. was playing only a support role. He gave his approval because he believed that, if he failed to do so,

[2] Quoted in Mr. Justice R.M. Hope, *Protective Security Review* (Canberra, 1979), p. 56.

relations between the R.C.M.P. and the two forces would suffer. To avoid these and other problems, we propose that the Director General or a deputy designated by him be informed of all joint operations. Of course, under the control system we have recommended joint operations involving the most intrusive techniques in investigation will also require ministerial approval. Moreover, general schemes of longer term co-operation between the security intelligence agency and provincial authorities should require ministerial approval. Before approving a joint operation the Director General should have at least the following information:

- an assessment of the target
- the reasons for the joint operation
- the resources each partner in the operation plans to commit
- the expected duration
- the organizational structure for the operation
- the type of investigative techniques to be used
- a plan for providing senior members of the security intelligence agency with periodic progress reports

26. Even these two types of prior approval may not be sufficient to avoid all of the serious pitfalls that a joint operation may present. For example, we would be concerned if the partners of the security intelligence agency in a joint operation rather than the agency itself took complete responsibility for employing intrusive investigative techniques. In this way, the agency would be receiving the intelligence and indeed participating in the management of the operation without having to go through the stringent control procedures which we have recommended in Chapter 4 of this part of our Report. To avoid this problem, we are of the view that the security intelligence agency should not use joint operations to circumvent control procedures for the use of covert intelligence-gathering methods. The Solicitor General should develop guidelines for the use of such methods in joint operations.

Relationships with provincial attorneys general and solicitors general

27. Co-operation in the past between federal and provincial authorities with security responsibilities has been of an *ad hoc* nature. We have already noted the situation regarding security screening for provincial or municipal authorities. Co-operation between the two levels of government, has, typically, been through two channels: from the federal Solicitor General to his provincial counterparts; and from the R.C.M.P. to the provincial attorney general. In total, however, there has been little co-operation of a systematic nature. In the autumn of 1977, at the close of the Federal-Provincial Conference of Attorneys General, a press communiqué was issued committing the Ministers responsible for police forces at both levels of government to close co-operation and co-ordination of intelligence-gathering in relation to organized crime. In response to this commitment, the R.C.M.P. canvassed all divisional Commanding Officers on the method and frequency of their communications with provincial attorneys general. The results showed a great diversity in the

frequency of contacts. While these contacts dealt principally with police matters, the Director General of the Security Service, Mr. Dare, directed that briefings of provincial authorities should also cover security matters of mutual concern such as terrorism. The briefings took place in the first half of 1978 and concentrated on areas where the Security Service's application of covert investigative techniques may have contravened provincial statutes. One result was that some of these techniques were discontinued pending clarification of their use by the attorneys general.

28. Our philosophy is that a spirit of federal-provincial co-operation should exist in the areas of policing and security. As stated at the beginning of this section, these areas will not benefit from a jealous guarding of jurisdictions. Indeed, many of our proposals are premised upon co-operation between the federal government and the provinces. Unilateral action cannot resolve many of the issues that we have examined throughout this Report. In the preceding paragraphs we have mentioned the need for systematic co-operation between the two levels of government through the use of written agreements covering such activities as security screening, V.I.P. security, and liaison between the security intelligence agency and provincial and municipal police forces. Similar co-operation is necessary in the effective handling of complaints alleging R.C.M.P. misconduct — a topic which we examine in Part X, Chapter 2. In addition, our analysis has shown that if the rule of law is to be strictly observed, neither the security intelligence agency nor criminal investigation agencies can effectively carry out their functions without amendments to provincial as well as federal laws. Thus there is a need for formal co-operation between the federal Solicitor General and the provincial attorneys general or solicitors general in obtaining the necessary legislative changes.

29. It is clear, therefore, that for both legal and operational reasons, the Solicitor General and his provincial counterparts should establish more effective procedures and mechanisms for federal-provincial co-operation in security matters. In this regard, we should note one further concern. It would be tragic for the future of Canadian democracy if, having brought security intelligence operations under an adequate system of control at the federal level, there were to emerge at the provincial level or in the private security industry organizations using operational techniques which encroach on liberal democratic principles and which are not subject to a rigorous system of democratic control. We are particularly concerned about the growth of the security industry in the private sector. There are now more private security personnel in Canada than there are policemen. A few large firms dominate the contract part of the industry and within such firms former members of the R.C.M.P. are prominent. There is some evidence that these former members retain close links with their former colleagues — links which may give them access to security information.[3] A prime concern in the expansion of private security forces is their effect on cherished freedoms in this country through, for example, their

[3] The expansion of the security industry in the private sector is outlined in Clifford D. Shearing and Philip C. Stenning, *Private Security and Law Enforcement in Canada*, a study prepared for the Department of the Solicitor General, December 1977.

possible use to infiltrate groups in order to prevent unionization. A similar growth in the private security industry is evident in the United States particularly since the reforms which have changed the scope of F.B.I. operations. We are disturbed by this trend and are convinced that effective co-operation between the federal and provincial authorities, including the security intelligence agency, must be established to monitor this development.

The reporting and investigation of alleged criminal activity committed by members or agents of the security intelligence agency

30. Two important questions concerning the relationship between federal and provincial governments arise when there is some indication that members or agents of the security intelligence agency have been engaged in acts that may be violations of the Criminal Code or other federal or provincial statutes. First, if knowledge of criminal activity first comes to the attention of the Solicitor General of Canada or some other federal Minister, should they be obliged to bring the matter to the attention of the prosecuting authorities in the province where the violation of the law has apparently occurred? Second, should there be any limitations on the access by provincial investigators to information held by the federal government which may relate to the alleged offences?

31. These are difficult questions and neither existing statute law nor judicial decisions provide full answers. These questions have not been submitted to a systematic analysis by provincial and federal authorities, nor are we aware of clearly defined solutions adopted by other federations. We think it will be essential for federal and provincial authorities to discuss these questions and to consider alternative solutions. The approach we suggest below is designed to strike a balance between provincial responsibility for the administration of justice and the paramount federal responsibility for protecting the security of Canada. As such, it avoids the extreme of giving either level of government an absolute and exclusive authority for investigating and directing criminal proceedings with respect to criminal activities by persons associated with the security intelligence agency. We hope that this proposal will be of assistance to those involved in federal-provincial consultations on this subject and we suggest that the approach we outline below be followed at least on an interim basis while a permanent system is being developed.

32. We think that the starting point for answering the questions we pose in this section must be recognition of the fact that traditionally in Canada the provinces have exercised the prime responsibility for instituting criminal proceedings. We are not concerned here with violations against the Official Secrets Act, which expressly makes prosecution subject to the approval of the Attorney General of Canada, or with the Narcotic Control Act, as to which the Supreme Court of Canada has held that there is concurrent federal and provincial jurisdiction to prosecute.[4] We also leave aside other federal statutes that create offences, such as the Income Tax Act and the Customs and Excise Act, jurisdiction over the enforcement of which has not in recent years been

[4] *R.* v. *Hauser* [1979] 1 S.C.R. 984.

vigorously asserted by the provinces. As far as federal legislation is concerned our discussion here relates only to violations of the Criminal Code.

33. The position traditionally taken by the provinces is that violations of the Criminal Code and of provincial statutes are matters relating to "the administration of justice in the province" and therefore are within provincial jurisdiction under section 92(14) of the British North America Act. There is, of course, no question that the enforcement of provincial statutes is a matter for the provinces. As for the Criminal Code, the provincial position is generally supported by constitutional authorities. One recent author summarizing judicial decisions on this issue states that:[5]

> The responsibility for the enforcement of the criminal law by police and prosecutors has been held to be within the provincial power over the administration of justice.[6] However, the federal Parliament has concurrent authority to provide for the enforcement of the criminal law on the basis that its legislative power over the criminal law (or any other subject matter) carries with it the matching power of enforcement.[7] In fact, however, the enforcement of the criminal law is for the most part carried out by the provinces.

Apart from Supreme Court decisions and statements of constitutional scholars on the law, we take cognizance of the policy statements of federal Ministers of Justice in the House of Commons to the effect that the prime responsibility for instituting proceedings with respect to Criminal Code offences rests with the provincial authorities.[8]

34. We see no reason for departing significantly from the tradition of provincial responsibility for criminal proceedings when it comes to offences by persons associated with Canada's security intelligence agency. On the contrary, precluding provincial responsibility for criminal law enforcement on the grounds that national security may be involved would conflict with the pattern of federal-provincial co-operation which, as we have recommended throughout this Report, should be the prevailing practice in national security matters.

35. Thus, when federal authorities become aware of possible criminal activities by members or agents of the security intelligence agency, the normal situation should be that the matter is brought to the attention of the appropriate provincial attorney general. It would then be up to police forces accountable to the provincial attorney general to proceed with the investigation and up to the provincial attorney general to decide whether or not to prosecute. We take exactly the same approach to the investigation and prosecution of criminal activity by members of the R.C.M.P. involved in criminal investigation work (see Part X, Chapter 2).

---

[5] Hogg, *Constitution of Canada*, Toronto, Carswell, 1977, pp. 277-8.

[6] Citing principally *Di Iorio* v. *Montreal Jail Warden* (1977) 73 D.L.R. (3d) 491 (Sup. Ct. Can.).

[7] Citing *Re Collins and the Queen* [1973] 2 O.R. 301, affirmed without reference to merits [1973] 3 O.R. 672 (Ont. C.A.); *R.* v. *Pelletier* [1974] 4 O.R. (2d) 677 (Ont. C.A.).

[8] These statements are discussed in J.Ll.J. Edwards, *Ministerial Responsibility for National Security*, Ottawa, 1980, pp. 14-15.

36. We think that the proper channel for communicating information to the provincial authorities about criminal activity by members or agents of the security intelligence agency is the Attorney General of Canada. Where federal authorities, such as the Legal Adviser to the security intelligence agency, or the Solicitor General as the Minister responsible for the agency, or the independent review body, (the Advisory Council on Security Intelligence which we recommend be established in Part VIII, Chapter 2), come across evidence pointing to criminal violations by members of the agency or by persons on behalf of the agency, they should bring the matter and *all* the evidence, pertaining to it to the attention of the Attorney General of Canada.

37. Once evidence of a criminal offence by a member or agent of the security intelligence agency is brought to the attention of the federal Attorney General, he should, subject to one exception, report the matter and the evidence pertaining to it to the attorney general of the province in which the alleged offence occurred. The one exception is a situation in which the Attorney General of Canada is convinced that national security, as defined in the Act governing the security agency, would be seriously damaged by turning over to the provincial authorites the evidence on which a decision to prosecute would have to be based. Such a decision by the Attorney General of Canada would be subject to a review procedure we will describe below. We stress that a decision not to report evidence of criminal activity to a provincial attorney general should only be made in highly exceptional circumstances by the law officer of the Crown at the federal level, applying the definition of national security in the statute governing the security intelligence agency and subject to an independent review process. The normal situation should be that such evidence is reported to the provincial attorney general so that the conduct of any ensuing investigation and the decision as to whether or not to lay charges may be made at the provincial level. This does not preclude federal authorities, including representatives of the security intelligence agency, discussing with the provincial attorney general the security implications of instituting criminal proceedings. But the decision as to whether or not to prosecute would normally be made by the provincial attorney general.

38. The second question we are concerned with may arise when, independently of reports from the federal Attorney General, the provincial attorney general receives information about a possible criminal offence by a member or agent of the federal security intelligence agency. What access will the provincial attorney general have to relevant information held by departments or agencies of the federal government? Let us be clear that we are discussing this question at the investigatory stage. Once a decision to prosecute is made and the case is before the courts, there are a number of laws such as section 41 of the Federal Court Act and rules concerning the protection of the identity of sources which may provide a legal basis for not disclosing certain information in judicial proceedings.[9] But we are concerned here with the position of the provincial attorney general before trial when he is trying to determine whether the evidence in his possession justifies laying a charge. At this stage he may well have reason to believe that important evidence which may have a vital bearing on the exercise of his prosecutorial discretion is in the hands of the federal

government. In these circumstances should there be any limitation on his access to information held by the federal government?

39. Again our answer to this question is that, in a situation of this kind, the governing principle should be that the federal authorities co-operate fully with the provincial attorney general and that, subject to one exception, the Attorney General of Canada should see to it that all the information possessed by the federal government pertinent to the alleged offence is disclosed to the provincial attorney general. The one exception to this principle of full disclosure is that there may be very exceptional circumstances in which the disclosure of certain information to provincial prosecutorial authorities would jeopardize the protection of national security as we have defined that concept in this Report. In these circumstances, and subject to a review process which we will enlarge upon below, we think the Attorney General of Canada should have the right to withhold information from a provincial attorney general. Recognition of this right is a necessary safeguard to ensure that the federal government can effectively discharge its paramount responsibility for protecting the security of Canada.

40. Setting some limit to the federal government's obligation to co-operate with provincial authorities in investigating criminal activity by members of the security intelligence agency is consonant with the basic tendency in our legal system to balance the need for effective law enforcement with the need to protect other important social values. The powers of investigating and prosecuting authorities in the Canadian legal system are not unlimited. For example, there is recognition at both the investigative and trial stages of our criminal justice system of the need to maintain the confidentiality of lawyer-client communications and, in the public sphere, section 41 of the Federal Court Act recognizes the right of a federal Minister to withhold information from court proceedings on a number of grounds including the danger of causing injury to national security. It would seem to us to be imprudent not to provide some protection for that latter interest at the investigatory stage of criminal proceedings. In taking this position, we should re-emphasize that the limit on provincial investigators' access to federal government information should apply only in exceptional circumstances.

---

[9] In our First Report, *Security and Information* (Ottawa, Department of Supply and Services, 1979), we recommended that "the provision of section 41(2) of the Federal Court Act not apply to security and intelligence documents or their contents and that new legislation be enacted providing that

(a) when a Minister of the Crown claims a privilege for such information on the grounds that its disclosure would be injurious to the security of Canada; or

(b) any person hearing any judicial proceedings is of the opinion that the giving of any evidence would be injurious to the security of Canada

the matter shall be referred to a judge of the Federal Court of Canada, designated by the Chief Justice of that court, to determine whether the giving of such evidence should be refused.

41. In a régime which strives to maintain federal-provincial co-operation in security matters such a restriction should rarely apply. But we can think of possible examples. For instance, some information on the security intelligence agency's files will have been obtained from foreign agencies on the firm understanding that it not be passed on to a third party. In the previous chapter we pointed out how essential it was for Canada's security intelligence agency to attach similar restrictions on information the Canadian agency provides to the national security agencies of other countries. We would think it wrong for the federal government to be required to turn over information to provincial investigators in circumstances that would violate the conditions under which information has been obtained from a foreign country. Another example is one in which the identity of a security intelligence informant who has penetrated a terrorist cell may be contained in records of security operations relating to a criminal offence which is being investigated by provincial authorities.

42. It is important that the federal decision not to report evidence of criminal activity to a provincial attorney general or to restrict the provincial attorney general's access to information be made as carefully as possible and be subject to review. Therefore, the Attorney General of Canada, as the Law Officer of the Crown at the federal level, should be responsible for making such decisions. He should be guided by a statutory standard which empowers him to withhold information if in his opinion disclosure of the information would seriously jeopardize the protection of Canada's national security as that concept is defined in the Act governing the security intelligence agency. In exercising his judgment the Attorney General of Canada should bear in mind that the governing principle favours co-operation with the provincial attorney general.

43. An independent review of the Attorney General's decision should be provided by the independent review body (the Advisory Council on Security and Intelligence). Full details of the information withheld should be reported to that body and, if it does not agree with the decision, it should so notify the Attorney General of Canada, and the Joint Parliamentary Committee on Security and Intelligence.

44. To increase the acceptability of the review process to the provinces, we think it would be wise to add provincial representatives to the Advisory Council on Security and Intelligence when it is reviewing decisions of the Attorney General of Canada. For this purpose the federal government should be able to supplement the membership of A.C.S.I. by three persons selected from a panel of seven persons nominated jointly by all the provincial attorneys general. Those persons should be bound by the same constraints as the regular members of the independent review body and therefore would not be permitted to disclose the information to which they are made privy, except to those persons to whom the independent review body may disclose it. We think that, even if the regular members of the independent review body do not decide that the matter should be the subject of comment and report to the Parliamentary Committee, it should nevertheless be the subject of such comment and report if such is desired by a majority of the provincial nominees.

WE RECOMMEND THAT the security intelligence agency and the R.C.M.P., with the approval of the Solicitor General, provide, upon request, security screening services

(a) to provincial governments for public service positions which have a bearing on the security of Canada;

(b) to provincial or municipal police forces.

(60)

WE RECOMMEND THAT the security screening services provided by the security intelligence agency for provinces and municipalities be subject to the same conditions which apply to the screening services for federal government departments and agencies.

(61)

WE RECOMMEND THAT, if the security intelligence agency obtains security relevant information about provincial politicians or public servants in the course of an investigation unrelated to a security screening programme for the Province in question, then the agency seek the approval of the Solicitor General before reporting this information to the appropriate provincial politician or official.

(62)

WE RECOMMEND THAT the Solicitor General encourage a provincial government which uses these security sceening services either to establish its own review procedures for security screening purposes or to opt into the federal government's review system.

(63)

WE RECOMMEND THAT the Solicitor General initiate a study of V.I.P. protection in foreign countries with federal systems of government with the aim of improving federal-provincial co-operation in this country.

(64)

WE RECOMMEND THAT the security intelligence agency, to facilitate the exchange of security relevant information with domestic police forces and generally to encourge co-operation,

(a) establish a special liaison unit for domestic police forces, staffed, in part, by personnel with police experience;

(b) develop written agreements with the major domestic police forces to include, among other things, the types of information to be exchanged, the liaison channels for effecting this exchange, and the conditions under which joint operations should be conducted.

(65)

WE RECOMMEND THAT the Director General approve all joint operations undertaken by the security intelligence agency and that the Solicitor General develop guidelines for the use and approval of intrusive investigative techniques in joint operations.

(66)

WE RECOMMEND THAT the Solicitor General develop in conjunction with his provincial counterparts a mechanism for monitoring the use by private security forces of investigative or other techniques which encroach on individual privacy, freedom of association, and other liberal democratic values.

(67)

WE RECOMMEND THAT

(a) **the federal government immediately initiate discussion with the provinces on the procedures which should apply to the reporting and investigation of criminal activity committed by members or agents of the security intelligence agency; and**

(b) **the arrangements outlined in this chapter be followed on an interim basis.**

(68)

PRIVY COUNCIL LIBRARY
BIBLIOTHÈQUE DU CONSEIL PRIVÉ
005231

DATE DUE

~~18/12/97~~		
~~9/4/98~~		
~~3/12/97~~		
~~18/6/99~~		
~~8/3/00~~		
~~3/05/2004~~		
~~7/09/2004~~		
~~Sept 20/04~~		
~~4/11/2004~~		
~~15/11/2004~~		
~~30/11/2004~~		
~~19/04/2006~~		
5/07/2006		

Brodart Co. Cat. # 55 137 001 Printed in USA

HV7641/.A3/C3/no.2-1
McDonald, D. C. (David C.)
Freedom and security under
the law : second
ACOW c. 1 aa PCO

