

Air India Flight 182
A Canadian Tragedy

VOLUME THREE
The Relationship Between Intelligence
and Evidence and the Challenges of
Terrorism Prosecutions

©Her Majesty the Queen in Right of Canada, represented by the
Minister of Public Works and Government Services, 2010

Cat. No: CP32-89/2-2010E
ISBN: 978-0-660-19926-9

Available through your local bookseller or through
Publishing and Depository Services
Public Works and Government Services Canada
Ottawa, Ontario
K1A 0S5

Telephone: (613) 941-5995 or 1 800 635-7943
Fax: (613) 954-5779 or 1 800 565-7757
Publications@pwgsc.gc.ca
Internet: www.publications.gc.ca

VOLUME THREE
THE RELATIONSHIP BETWEEN
INTELLIGENCE AND EVIDENCE
AND THE CHALLENGES OF TERRORISM PROSECUTIONS

TABLE OF CONTENTS

CHAPTER I: INTRODUCTION	11
1.0 Tension between Secrecy and Openness	12
1.1 Resolving the Tension	13
CHAPTER II: COORDINATING THE INTELLIGENCE/EVIDENCE RELATIONSHIP	17
2.0 Introduction	17
2.1 The Need to Revise the Approach to Preventing Terrorism	19
2.2 The Critical Role of CSIS in Providing Intelligence to Government about Security Threats	21
2.2.1 Inherent Tensions between CSIS and the RCMP	22
2.2.2 Joint Management Team Meetings	23
2.3 The Current Role of the National Security Advisor	26
2.3.1 Competing Views on the Adequacy of the Coordination Powers of the National Security Advisor	28
2.3.2 The Legitimate Role of the Prime Minister and the Privy Council Office in Coordinating National Security Activities	32
2.3.3 Expanding the Role of the National Security Advisor	34
2.3.3.1 <i>Establishing Strategic National Security Policies and Priorities</i>	35
2.3.3.2 <i>Coordination of National Security Activities, Including Distribution of Intelligence</i>	37
2.3.3.3 <i>The Need for a Privilege to Protect the NSA's Deliberations and Information Received by the NSA</i>	38
2.3.3.4 <i>The Relationship between the NSA and CSIS</i>	40
2.3.3.5 <i>The Relationship between the NSA and Law Enforcement Agencies</i>	40
2.3.3.6 <i>Resolving Disputes between the Agencies, Including Disputes Arising from the Intelligence/Evidence Relationship</i>	41

2.3.3.7	<i>Oversight of the Effectiveness of National Security Activities</i>	42
2.3.3.8	<i>Staffing the National Security Advisor's Office</i>	44
2.3.3.9	<i>Limits on the Role of the National Security Advisor: No Direct Budgetary or Personnel Control and Limited Operational Involvement</i>	45
2.3.3.10	<i>International Best Practices on Central Coordination of National Security Activities</i>	45
2.3.3.11	<i>Summary of the National Security Advisor's Enhanced Role</i>	46
CHAPTER III: COORDINATING TERRORISM PROSECUTIONS		49
3.0	Introduction	49
3.1	Limits on Police Discretion in Terrorism Investigations and Prosecutions	50
3.2	The Role of Prosecutorial Discretion in Terrorism Cases	54
3.3	The Role of the Federal Director of Public Prosecutions in Terrorism Prosecutions	57
3.3.1	The Need for a Specialized Director of Terrorism Prosecutions	58
3.3.2	The Role of Provincial and Territorial Attorneys General in Terrorism Prosecutions	62
3.3.3	The Need for Provincial Authorities to Notify Federal Authorities about Possible Terrorism Prosecutions	63
CHAPTER IV: THE COLLECTION AND RETENTION OF INTELLIGENCE: MODERNIZING THE CSIS ACT		65
4.0	Introduction	65
4.1	No Absolute Secrecy and No Wall between Intelligence and Evidence	66
4.2	Section 12 of the <i>CSIS Act</i> , the Collection and Retention of Intelligence and the Implications of <i>Charkaoui v. Canada</i>	69
4.2.1	The Destruction of Intelligence in the Air India Investigation	69
4.2.2	Interpreting Section 12 of the <i>CSIS Act</i>	72
4.2.3	The Supreme Court of Canada's Interpretation of Section 12 of the <i>CSIS Act</i> in <i>Charkaoui</i>	73
4.2.4	The Need for New CSIS Policies on Retention of Intelligence	75
4.2.5	Conditions for the Collection of Intelligence	77
4.3	Privacy Issues	79

4.4	Section 19 of the <i>CSIS Act</i> and the Distribution of Intelligence	81
4.4.1	CSIS Discretion under Section 19(2)(a) Not to Share Relevant Information with the Police	82
4.4.2	Rationales for CSIS Discretion Not to Give the Police Relevant Information	83
4.4.3	Submissions on CSIS Discretion to Share Information with the Police	85
4.4.4	The Commission's Proposed Approach to Information Sharing	86
4.4.5	The Role of the National Security Advisor in Sharing CSIS Information	89
4.5	Culture Change within CSIS: Beyond "We Don't Collect Evidence"	91
4.6	Culture Change in the RCMP: Beyond "The Less Information We Receive from CSIS, the Better"	97
4.7	Using CSIS Information in a Criminal Trial: Section 21 of the <i>CSIS Act</i>	99
4.7.1	The Important and Expanded Role of <i>Criminal Code</i> Electronic Surveillance in Terrorism Investigations	101
4.7.2	Electronic Surveillance Outside Canada	103
4.7.3	Reconciling Secrecy and Disclosure in Allowing Warrants to Be Challenged: The Current Editing Solution	104
4.7.4	The Use of Special Advocates in Proceedings to Challenge <i>CSIS Act</i> and <i>Criminal Code</i> Warrants	105

CHAPTER V: THE DISCLOSURE AND PRODUCTION OF INTELLIGENCE 109

5.0	Introduction	109
5.1	Disclosure of Information	109
5.2	Retention of Information	114
5.3	The "Relevance" Requirement	115
5.4	Applying <i>Stinchcombe</i> to Intelligence	116
5.4.1	The Role of <i>Stinchcombe</i> in the Air India Prosecutions	117
5.4.2	The Effect of <i>Stinchcombe</i> on CSIS/RCMP Cooperation	117
5.5	Potential Changes to the Approach to Disclosure	119
5.6	The Need for Guidelines on the Proper Extent of Disclosure	122
5.7	Production of Intelligence under <i>R. v. O'Connor</i>	124
5.7.1	Legislating Requests for Production of Intelligence under <i>O'Connor</i>	125
5.8	Anticipating Disclosure	126

CHAPTER VI: THE ROLE OF PRIVILEGES IN PREVENTING THE DISCLOSURE OF INTELLIGENCE 127

6.0	Introduction	127
6.1	The Role of Police Informer Privilege in Terrorism Investigations and Prosecutions	128

6.1.1	Loss of Informer Privilege When the Informer Is or Becomes an Agent or Material Witness	131
6.2	Informer Privilege and the Transfer of Sources from CSIS to the RCMP	133
6.3	Should CSIS Informers Be Protected by Informer Privilege	135
6.4	Are New National Security Privileges Necessary	140
6.4.1	Cabinet Confidences	141
6.4.2	A New National Security Privilege for Deliberations of the National Security Advisor	142

CHAPTER VII: JUDICIAL PROCEDURES TO OBTAIN NON-DISCLOSURE ORDERS IN INDIVIDUAL CASES 145

7.0	Introduction	145
7.1	Section 37 of the <i>Canada Evidence Act</i>	147
7.2	Section 38 of the <i>Canada Evidence Act</i>	149
7.2.1	The Importance of Section 38 Proceedings in Terrorism Investigations and Prosecutions	151
7.2.2	Avoiding Section 38 Proceedings in the Air India Prosecutions	152
7.2.3	Other Experiences with Section 38 of the <i>Canada Evidence Act</i>	153
7.2.4	Procedures Equivalent to Section 38 in Other Countries	156
7.2.5	Submissions to the Commission about the Two-Court System under Section 38	158
7.3	Is the Two-Court Approach Sustainable	160
7.4	Which Court is Best Suited to Conduct Terrorism Trials and Decide Issues of National Security Confidentiality	163
7.5	Appeals before the Completion of Terrorism Trials	165
7.6	Possible Use of Special Advocates in Section 38 Proceedings	167
7.7	The Problems Created by Overstating the Need for Secrecy	170
7.7.1	Towards a More Disciplined and Harm-based Approach to Claims of Secrecy	172
7.8	Evolving National Security Confidentiality Jurisprudence	174
7.9	The Ultimate Responsibility of the Attorney General of Canada with Respect to Disclosure of Intelligence	177

CHAPTER VIII: MANAGING THE CONSEQUENCES OF DISCLOSURE: WITNESS AND SOURCE PROTECTION 179

8.0	Introduction	179
8.1	Terminology	180
8.2	Why Witness Protection	181
8.3	Witness Intimidation and its Impact on Terrorism Investigations and Prosecutions	184
8.3.1	The Context of Terrorism	184

8.3.2	Exploiting the Particular Vulnerabilities of Some Communities – “Community-wide” Intimidation	184
8.3.3	How Distrust and Distance Limit the Ability of Authorities to Provide Protection	188
8.3.4	Examples of Individual and Community-wide Intimidation in the Air India Context	189
8.3.5	Intimidation of Members of the Sikh Community for Speaking Out”	191
8.3.6	Reducing Intimidation and Promoting Trust	194
8.3.7	Witness Protection during the Air India Investigation	195
8.3.8	Conclusion	197
8.4	Protecting Identity to Avoid the Need for Witness Protection	198
8.4.1	The Role of Prosecutorial Discretion	199
8.4.2	Editing Affidavits Prepared in Support of Applications Warrants	200
8.4.3	Relying on Police Informer Privilege	200
8.4.4	Disclosure: Non-relevance and Timing	203
8.4.5	Sections 37 and 38 of the <i>Canada Evidence Act</i>	203
8.4.6	“Partial Anonymity”	204
8.4.7	Conclusion	206
8.5	Anonymous Testimony	207
8.5.1	The British Experience with Anonymous Testimony	210
8.5.2	Anonymous Testimony and the Adversarial System	213
8.5.3	Anonymous Testimony and the <i>Charter</i>	214
	8.5.3.1 <i>No Right to Physical Confrontation of a Witness but a Right to Have an Opportunity to Engage in Cross-Examination</i>	215
	8.5.3.2 <i>Anonymous Testimony and the Right of Cross-Examination</i>	215
	8.5.3.3 <i>Section 7 of the Charter and Anonymous Witnesses</i>	217
	8.5.3.4 <i>Section 1 of the Charter</i>	217
8.5.4	Conclusion	220
8.6	Witness Protection Programs	221
8.6.1	Responsibility for Protecting Witnesses	222
8.6.2	The Federal Witness Protection Program	222
8.6.3	Hardships Related to Living in the WPP	224
8.6.4	Additional Challenges of Living in the WPP in Terrorism Matters	227
	8.6.4.1 <i>Minority Communities</i>	227
	8.6.4.2 <i>Lack of WPP Benefits beyond Protection</i>	228
8.6.5	Alternative Measures to Protect Witnesses	229
8.6.6	Organizational Problems in the WPP	231
	8.6.6.1 <i>The Need to Consider the Interests of All Parties in Terrorism Prosecutions</i>	231
	8.6.6.2 <i>Lack of Firewall between Investigative Units and the WPP</i>	232
	8.6.6.3 <i>Inadequate Conflict Resolution Mechanisms</i>	233

8.6.6.4	<i>The Need to Restructure the WPP in Terrorism Matters</i>	234
8.6.7	A New Body to Manage Witness Protection: A National Security Witness Protection Coordinator	235
8.6.7.1	<i>Judicial Review of the National Security Witness Protection Coordinator's Decisions</i>	241
8.6.7.2	<i>The Decision to Admit or Refuse Entry to Witness Protection</i>	241
8.6.7.3	<i>Dispute Resolution</i>	242
8.6.8	Other Issues Relating to Witness Protection in Terrorism Cases	245
8.6.8.1	<i>International Agreements</i>	245
8.6.8.2	<i>Independent Legal Advice for Protectees</i>	246
8.6.8.3	<i>Psychological Evaluations</i>	247
8.6.8.4	<i>Witnesses who are Minors</i>	248
8.6.8.5	<i>Collaborators who are Inmates</i>	249
8.6.8.6	<i>Investigative Hearings</i>	251
8.7	Conclusion	254

**CHAPTER IX: MANAGING THE CONSEQUENCES OF DISCLOSURE:
THE AIR INDIA TRIAL AND THE MANAGEMENT OF OTHER COMPLEX
TERRORISM PROSECUTIONS** 257

9.0	Introduction	257
9.1	The Challenges of Terrorism Prosecutions	262
9.2	The Air India Criminal Trial	265
9.2.1	Project Management	269
9.2.2	The Disclosure Process	270
9.2.3	Services for Family Members of Flight 182 Victims	273
9.2.4	Trial Costs	276
9.2.5	Federal-Provincial Cost-sharing	278
9.3	Making Terrorism Trials Workable	279
9.3.1	Project Management	281
9.3.2	Cost-sharing	281
9.3.3	The Trial Judge	281
9.3.4	Defence and Crown Counsel	283
9.3.4.1	<i>Funding</i>	283
9.3.4.2	<i>Conduct of Counsel</i>	287
9.3.5	Accountability of the Legal Profession for Trial Delays	289
9.3.5.1	<i>Lawyers</i>	289
9.3.5.2	<i>Judges</i>	290
9.3.6	Pre-trial Motions	297
9.3.7	Pre-trial Conferences	301
9.3.8	Reducing Delays and Re-litigation Caused by Severance Orders and Mistrials	303
9.4	Disclosure	307
9.4.1	Electronic Disclosure	308
9.4.2	Staged Disclosure	310

9.4.3	Disclosure Issues Relating to Section 38 of the <i>Canada Evidence Act</i>	312
9.4.4	Late and Continuing Disclosure	313
9.5	Issues at Trial	314
9.5.1	Inability of the Trial Judge to Continue	314
9.5.2	The Jury	316
	9.5.2.1 <i>Avoiding Mistrials Caused by Discharge of Jurors</i>	320
9.5.3	Three-judge Panels	323
9.5.4	Mandatory Jury Trials	329
9.5.5	Addressing the Needs of Victims	331
9.6	Conclusion	331
	CHAPTER X: RECOMMENDATIONS	333

Volume Three: The Relationship Between Intelligence and Evidence

VOLUME THREE

THE RELATIONSHIP BETWEEN INTELLIGENCE AND EVIDENCE AND THE CHALLENGES OF TERRORISM PROSECUTIONS

CHAPTER I: INTRODUCTION

The success of counterterrorism efforts depends on the ability of the government to recognize terrorist threats at an early stage and to respond rapidly with appropriate measures. Secret intelligence can help the government to recognize those threats. Typically, an intelligence agency, Canadian or foreign, and not the police, will acquire such intelligence first.

Deciding when and how to respond to a terrorist threat is among the most important decisions of any government. Making the right decision requires an understanding of available responses and an assessment of the suitability of each to combat the threat.

The appropriate response by government must begin with an understanding that each terrorist threat is unique and that government actions must be tailored to reflect this. There is no presumptively “best” response. To deal with one terrorist threat, it may be appropriate to engage the police; to deal with another, it may be best to rely on actions by immigration authorities or to pass information to foreign agencies to help them deal with the threat from abroad. Sophisticated, flexible decision making is needed.

Canadian efforts against terrorism involve many disparate entities, including the Canadian Security Intelligence Service (CSIS), the Royal Canadian Mounted Police (RCMP), the Department of Foreign Affairs and International Trade (DFAIT), the Canada Border Services Agency (CBSA) and the Communications Security Establishment (CSE). Each agency¹ has its own mandate and rules governing how it carries out that mandate. CSIS has a mandate to collect intelligence to inform the government about threats to the security of Canada.² The RCMP has primary responsibility for preventing and investigating crimes that constitute a threat to the security of Canada.³

This volume evaluates how effectively the government uses the resources that are available to it to deal with the terrorist threat. It also addresses how best

¹ The term “agency” here refers both to departments and to agencies.

² *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23.

³ *Royal Canadian Mounted Police Act*, R.S.C. 1985, c. R-10; *Security Offences Act*, R.S.C. 1985, c. S-7, s. 6.

to manage the flow of information between government agencies in terrorism matters – most often, the flow of information between CSIS and the RCMP.

1.0 Tension between Secrecy and Openness

Police investigations and criminal prosecutions remain a central feature of Canada's response to terrorism. However, involving law enforcement agencies introduces potential difficulties. Chief among them are legal restrictions that prevent the police and the justice system from using intelligence from agencies such as CSIS while maintaining the secrecy of that intelligence. Any proposed use of intelligence as evidence in a criminal investigation or trial – the "intelligence-as-evidence" phenomenon – encounters tension between the need for secrecy within the intelligence community and the need for openness in the criminal investigative and trial processes. This tension reveals the differences between how the police and intelligence communities do their work.

Security intelligence agencies have a statutory mandate to inform the government about security threats. They often rely on secrecy to protect human sources, ongoing investigations and the confidentiality of intelligence that foreign agencies have shared. The further disclosure of intelligence can compromise a security agency's effectiveness. This need for secrecy results in a desire by intelligence agencies such as CSIS to minimize the disclosure of intelligence to the RCMP for criminal investigations.

In contrast, police forces generally collect information about crimes in the expectation that the information will be disclosed to the accused and relied upon in public trials. Police forces therefore seek out witnesses who have no concern about testifying or about supplying information that can be introduced in public trials. It is of little use to the police to use secret information in criminal investigations if that information cannot be used in court.

This tension between secrecy and openness is particularly pronounced in counterterrorism matters because of the overlapping mandates of the RCMP and CSIS. CSIS and the RCMP are each legitimately involved in investigating the same activities. Terrorism is both a threat to Canada's security and a crime. As a threat to national security, terrorism falls squarely within the core mandate of CSIS. As a crime, terrorism falls squarely within the RCMP mandate to investigate and prosecute crime. The overlap increased with the enactment of the *Anti-terrorism Act*⁴ in 2001. Terrorism offences now include the planning of, and the provision of assistance for, terrorist acts, whether or not the acts occur. As a result, the RCMP is now involved in investigating an increasing number of terrorism matters that, before the *Anti-terrorism Act*, were largely addressed by CSIS without police involvement.

⁴ S.C. 2001, c. 41.

1.1 Resolving the Tension

This volume proposes how to resolve the tensions that arise when CSIS and the RCMP occupy the same territory. At present, there is no effective and independent decision maker, charged with ensuring that responses to terrorism issues serve the broad public interest and not merely the sometimes narrower interests of individual agencies.

As one solution, the Commission recommends that the office of the National Security Advisor (NSA) be given an expanded role, before any police involvement, in managing terrorist threats. In part, this role would see the NSA deciding whether it is possible to respond to a given threat without involving criminal investigations and prosecutions that might lead to the public disclosure of secret information. In other cases, if CSIS hesitates, or is unwilling, to pass information to the RCMP, the NSA should have the power to require CSIS to provide the information. In these and other situations, the NSA will act in the public interest, transcending institutional self-interest. It is impossible to resolve these enduring tensions completely. Nevertheless, the manner in which decisions are made about the appropriate balance between secrecy and openness can be improved.

Criminal prosecutions are not the only way to respond to terrorism, but they have distinctive abilities to incapacitate, punish and denounce the guilty. At the same time, these prosecutions face challenges. These challenges are the product of the need to decide what intelligence can remain secret and what must be used or disclosed in a criminal trial. Other concerns relate to managing the quantity of disclosure and multiple pre-trial motions, the sustainability of juries in long trials and the need to protect witnesses from intimidation.

The terms of reference require the Commission to make findings and recommendations about "...establishing a reliable and workable relationship between security intelligence and evidence that can be used in a criminal trial."⁵ The focus of this aspect of the Commission's work has been on building appropriate decision-making processes, from the initial collection of intelligence through to its distribution within government and its possible use in legal proceedings.

There is an absolute need for an efficient, fair process in a criminal proceeding to adjudicate claims by government that intelligence should be kept secret⁶ and, if so, whether that intelligence is subject to disclosure to ensure that the accused receives a fair trial. The Commission recommends in this volume that the judge presiding over the criminal trial be permitted to adjudicate any claim made by the government to prevent intelligence from being disclosed publicly. This would replace the present system, which involves proceedings before two

⁵ Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, Terms of Reference, P.C. 2006-293, para. b(iii) [Terms of Reference].

⁶ This involves litigation under s. 38 of the *Canada Evidence Act*, R.S.C. 1985, c. C-5.

different judges in two separate court systems, with each judge in possession of only part of the information necessary to make the decision. All this now occurs without representation for the accused and without the accused being informed of the content of the secret information. Under the system proposed by the Commission, the trial judge would make decisions about privilege and about its impact on the fairness of the proceedings, and would have access to all information relevant to making those decisions.

To ensure fairness in the criminal process, accused persons should be represented at the hearing that determines whether the information should be kept secret. At present, only government lawyers are present at such hearings. In this volume, the Commission recommends that special advocates be allowed to represent the interests of the accused, and that a process be used similar to that for immigration proceedings involving security certificates.

This volume also addresses other challenges of terrorism prosecutions, most notably the difficulties posed for the state by the obligation to disclose to the accused what may be huge volumes of material, and the trial delays stemming from multiple pre-trial motions. The volume discusses how judges can manage the pre-trial process more firmly to ensure that terrorism cases do not collapse before a trial can be held on the merits. Better management of the pre-trial process by judges will be increasingly important, since the amount of disclosure in terrorism cases is likely to grow as domestic and foreign intelligence agencies work more closely with the police, producing greater amounts of information that will be subject to disclosure requirements.

Long trials are difficult for juries and raise the prospect of mistrials if too many jurors have to be excused during the trial. This volume addresses various suggestions for resolving the problems that arise with lengthy jury trials, including empanelling additional jurors, reducing the number of jurors required to reach a verdict, or using a panel of three judges, without a jury, to hear terrorism cases.⁷

Reforms are needed in how criminal cases are prosecuted. It is wasteful and inefficient to have separate agencies involved in discrete aspects of terrorism prosecutions. At present, each agency is represented by counsel, and national security privilege litigation is conducted by counsel other than the prosecutor. Instead, one unit should be responsible for dealing with all aspects of a terrorism prosecution, from managing the relationship between government agencies to conducting national security privilege litigation. The role of this unit should include providing legal support to law enforcement agencies as well as ensuring that the secrecy of intelligence operations is maintained and that rules governing the disclosure of information to the accused are followed. The Commission calls for the appointment of a Director of Terrorism Prosecutions, who would serve under the Attorney General of Canada and whose office would be staffed by prosecutors with expertise in national security matters.

⁷ Terms of Reference, para. b(vi).

Converting intelligence into evidence involves the management of human sources – specifically, dealing with how, and under what circumstances, they may become witnesses in criminal prosecutions. A tension exists between the need to provide confidentiality to sources and the fact that, if sources are used in criminal prosecutions, their identities will become known through disclosure to the defence and through giving evidence in public at trial. Difficulties in transferring sources from CSIS to the RCMP were a constant problem in the post-bombing Air India investigations, and adequately protecting witnesses from intimidation was a serious concern during the Air India prosecution.

Witness protection programs were instituted to protect witnesses from harm if their identities became known. At present, admission to such programs is controlled by the RCMP. Decisions about extending witness protection should not be made by an agency with an interest in ensuring that sources agree to become witnesses. In this volume, the Commission recommends that responsibility for decisions about allowing individuals to enter witness protection programs should be transferred to a new agency.

This volume also addresses whether “police informer privilege” should be extended to CSIS sources. The issue is not as straightforward as it might at first seem. Extending this extremely robust privilege to CSIS sources would allow CSIS unilaterally to offer a privilege that would prevent its sources from being required, or even from being able to agree, to testify as witnesses. Just as it is inappropriate to have the police make protection decisions that prejudge the relative value of trial witnesses versus intelligence sources, it is inappropriate to give CSIS the unilateral ability to disqualify persons from becoming witnesses by extending the police informer privilege to them.

Still, CSIS sources should in some cases have their identities protected against disclosure. The common law recognizes a privilege that protects the confidentiality of information if it is in the public interest to foster the type of relationship in which the confidential information was disclosed. This “Wigmore privilege” has been interpreted to protect the identities of human sources, especially when they rely on CSIS promises of anonymity. Unlike the “police informer privilege,” however, reliance on the Wigmore privilege in a case may be reviewed by the courts to ensure that reliance on the privilege serves the public interest.

This volume shows how a just balance between secrecy and openness can be achieved by using an impartial decision maker at critical stages, such as when determining the appropriate response on learning of a terrorist threat or when assessing the need for secrecy and for the protection of sources and witnesses. The overriding theme is the need to establish clear responsibility and accountability for decisions in national security matters. What must be avoided is a diffusion of responsibilities, where each agency and each official acts properly but where they fail collectively to achieve the ultimate goal: protecting the

security of Canadians to the greatest extent possible. Promises by agencies to cooperate with each other are only part of the answer. Better rules, supported by legislation, are required. Even the best of intentions alone will not ensure an appropriate transition from intelligence to evidence.