Air India Flight 182

A Canadian Tragedy

VOLUME THREE

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

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

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 agency[1] 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 secret[6] 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.