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 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.

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

CHAPTER II: COORDINATING THE INTELLIGENCE/EVIDENCE RELATIONSHIP

2.0 Introduction

Since 9/11 there has been an increased need to establish strategic policy and priorities and to improve coordination between departments of government as more of them take on national security responsibilities. There has been an even greater need for decisive action to ensure coordination and proper sharing of information within government about potential security threats and terrorism.

Yet as more government agencies become involved in national security matters, there is an increased risk of bureaucratic fencing among them. Someone must be in charge to ensure that the agencies are executing the government's strategic security plans. Someone must also be in charge to ensure that disputes among agencies are resolved in the public interest. Someone must exercise meaningful oversight and have the power and legitimacy to intervene if the agencies are not cooperating or if the system is not effective. That person should be a guardian of the public interest – an interest that transcends those of individual agencies.

This chapter examines means of coordinating the government's response to the threat of terrorism, with particular attention to problems presented by the relationship between intelligence and evidence. Decisions on how and when to respond to a particular threat to national security should be taken in the public interest. In the Canadian context, the office of the National Security Advisor (NSA) is best positioned to carry out that task. This chapter advances the case for an enhanced role for the NSA.

The enhanced role for the NSA would give effect to the following policy imperatives:

- Where CSIS has determined that it should pass information to the RCMP, it should be free to do so without restraint and without the involvement of the NSA. This maximizes the development of expertise and enhances the improving relations between CSIS and the RCMP in terrorism investigations. This relationship should be encouraged to develop and mature;

- It is in Canada's national interest to protect some intelligence from the risk of public exposure that may flow from engaging the police. However, CSIS should not unilaterally decide to withhold information from the RCMP. Such decisions should be made by the NSA on behalf of the Prime Minister. This supervisory role would ensure that the decision to withhold information from the RCMP is made in the public interest;

- Some threats to national security can be managed effectively by employing alternatives to engaging the RCMP. Where there are good reasons not to engage the RCMP, those alternatives should be considered by the NSA;

- It is not the role of the NSA to supervise agencies, but to resolve disputes between those agencies.

During this Inquiry it became apparent that the obstacles to effective information sharing between CSIS and the RCMP, and to the successful conversion of intelligence into evidence, were symptomatic of a larger structural problem. Many agencies deal with national security issues under their mandates. These agencies are spread across various ministries and are not subject to an overriding line of authority for those national security matters.

There is no single agency at present with responsibility for managing, executing and controlling responses to terrorist threats. No one is in charge. Twenty-four years after the terrorist attack on Flight 182, there remains a worrying lack of integration and coordination among government agencies on national security matters.

In the vast majority of cases involving terrorist threats, CSIS monopolizes most aspects of the initial response. By gathering intelligence, CSIS assesses the extent of the threat and also determines the extent to which other partners will become involved in managing the threat. CSIS does this through its discretion about whether to disclose information to the RCMP or to other government agencies.[1] This leaves CSIS with the *de facto* ability to determine the *how* and the *when* of the government response to a threat. Dictating the government's response by controlling the flow of relevant information exceeds CSIS's statutory mandate. That mandate is to "report to and advise" the Government of Canada about threats to the security of Canada. The Government of Canada, not CSIS, is to decide the appropriate response.

CSIS should have sufficient tools to be able to learn of terrorist threats, even at their earliest stages. This is a different function from that of law enforcement

---

1 This is the result of the information sharing mandate set out in s. 19 of the *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23 [*CSIS Act*]. As discussed in Chapter IV, s.19(2)(a) gives CSIS discretion whether to disclose intelligence to police and prosecutors. Section 19(2) also gives CSIS discretion whether to disclose intelligence to ministers, such as the Minister of Foreign Affairs or the Minister of National Defence.

agencies and it should remain distinct.[2] CSIS is, in effect, stationed on a watchtower searching the horizon for early signs of danger. However, if CSIS does not inform the Government about the security threats that it sees on the horizon, no one in government except CSIS will know of them. CSIS will arrogate to itself the power to decide the Government's response to those threats. Yet it is the Prime Minister who must have the power and the ultimate responsibility to act for the Government of Canada in deciding how to respond to security threats. In discharging this responsibility, the Prime Minister is assisted by the NSA and by other non-partisan and expert public servants in the Privy Council Office.

The role of the Prime Minister in matters of national security is fundamental. If an act of terrorism occurs, the Prime Minister will have to answer to Parliament and to the people of Canada. The ultimate responsibility of the Prime Minister for national security is not a new and controversial theory of governance, nor a new and controversial invention for intelligence coordination. It has long been recognized and is a practical reality.[3]

2.1 The Need to Revise the Approach to Preventing Terrorism

There are some disadvantages to employing law enforcement as a tool to prevent terrorism. Chief among them is the inflexibility of the criminal trial process. Criminal investigations are time-consuming and expensive. So too are criminal trials. They both can attract publicity that may not be in the public interest. Moreover, there is a risk that the prosecutors will not be able to protect the confidentiality of information they receive from CSIS. As well, an unsuccessful prosecution can undermine confidence in a counterterrorism effort, even though it may simply represent the inability of the prosecution to meet the high standard of proof of guilt beyond a reasonable doubt. The decision to involve law enforcement must take into account these risks and any alternatives to a prosecution.

The RCMP is not always the only, or the best, agency to respond to a terrorist threat. For example, when dealing with non-citizens, the security certificate regime is, in some respects, preferable to the criminal law process because the government is able to rely on secret intelligence information to support the removal from Canada of persons who are a threat to national security.

---

2 Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (Ottawa: Public Works and Government Services Canada, 2006), pp. 312-316 [*Report of the Events Relating to Maher Arar: Analysis and Recommendations*].

3 *Report of the Royal Commission on Security* (Abridged) (Ottawa: Supply and Services Canada, 1969) [*Report of the Royal Commission on Security*]; Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Freedom and Security under the Law*, Second Report - vol. 2 (Ottawa: Supply and Services Canada, 1981), p. 847 [Freedom and Security under the Law]; Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (Ottawa: Public Works and Government Services Canada, 2006), p. 196 [*A New Review Mechanism for the RCMP's National Security Activities*].

Law enforcement, while not the only option, is a valuable and integral part of any nation's security machinery. Law enforcement offers unique means to denounce, disrupt and punish terrorism. Nevertheless, the involvement of law enforcement agencies must be the product of a considered and strategic decision, since it is not possible to rely on secret information to secure a conviction in a criminal trial.

A broad approach to the management of terrorist threats should be the norm. In cases of terrorist financing, for example, removing the charitable status of an organization may impair its ability to raise funds. It is also possible for the authorities to seek orders freezing or confiscating the assets of a terrorist organization. Preventive target-hardening measures may also be appropriate in areas such as aviation security. Given the international nature of terrorism, providing intelligence to allies may also reduce the threat within Canada.[4]

Terrorist threats engage the mandates of the RCMP, CSIS and, among others, the CBSA, the Department of National Defence (DND), the Department of Citizenship and Immigration, the Canada Revenue Agency (CRA), the Canadian Air Transport Security Authority (CATSA) and the Department of Foreign Affairs and International Trade (DFAIT). At present, the Minister of Public Safety is responsible for the nation's security, yet has authority only over CSIS, the RCMP and the CBSA. While much of the national security work is carried on in those agencies, they do not comprise all the agencies at the government's disposal. As Commissioner O'Connor noted, in reporting on the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, there are at least 25 government entities involved in national security matters, with 16 different departments and agencies being identified by the government as having "key" national security responsibilities.[5]

A flexible approach is needed to determine the appropriate governmental response. An NSA with enhanced responsibilities should perform a central role in deciding the appropriate response to particular security threats. The new governance structures proposed in this volume should allow for informed decisions about the costs and benefits of commencing terrorism prosecutions. They should also provide a forum for quick and decisive resolution of disputes that may arise between agencies.

The challenges of designing workable governance structures are significant but achievable. There must be respect for the principles of prosecutorial and police independence that are supported by the Canadian constitution and a corresponding commitment to the impartial application of the rule of

---

4 Although two recent commissions found deficiencies in information-sharing with other countries and recommended enhanced safeguards, both affirmed that this practice is an important tool to prevent terrorism. See *Report of the Events Relating to Maher Arar: Analysis and Recommendations*, pp. 320-321, 331-332, 343-349; *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin* (Ottawa: Public Works and Government Services Canada, 2008), pp. 68-71, 78, 81-93.

5 *A New Review Mechanism for the RCMP's National Security Activities*, pp.127-128.

law. There must be respect for the importance of maintaining secrets, but governance structures must prevent agencies with relevant information from withholding information from other agencies for fear that it will ultimately have to be disclosed publicly. Finally, there must be adherence to the constitutional protections for all individuals charged with criminal offences.

Any new governance structure must be nimble enough to allow quick decisions about imminent threats and must avoid duplicating existing bureaucracies. The structure must also avoid becoming a dysfunctional system in which each agency arguably does its own job properly while the system as a whole fails to achieve the ultimate objective of protecting the security of Canadians. To ensure that the system works to prevent terrorism, there must be someone at the centre of government to receive all relevant information and to make decisions in the public interest about the appropriate government response to particular security threats.

2.2 The Critical Role of CSIS in Providing Intelligence to Government about Security Threats

The CSIS mandate includes advising the Government of Canada about threats to Canada's security. CSIS does not have the mandate to prevent terrorist acts. It is not the responsibility of CSIS to carry out any law enforcement activities to prevent terrorism. CSIS provides advice; the Government is responsible for devising the appropriate response.

CSIS carries out operations in the sense that it conducts interviews, uses human sources, performs searches authorized by warrant, and clandestinely intercepts private communications.[6] All these are means by which CSIS obtains information to learn of threats to Canada's security. However, this operational mandate ceases after the information-gathering stage. Beyond that point, CSIS is not authorized to perform any "police-like" functions. For example, the *CSIS Act*[7] does not empower CSIS employees to conduct arrests, engage in disruption interviews, detain persons for interviews or employ agents (as opposed to sources, who merely provide information but do not become actively involved on behalf of CSIS in operations). Those techniques are reserved for other agencies, such as law enforcement and the Canada Border Services Agency (CBSA).

There is a transition from collecting intelligence to collecting evidence, as an operation shifts from an intelligence-gathering exercise to a law enforcement investigation. An obvious role for the NSA will be to ease the transition from intelligence to evidence.

The evidence at the Inquiry showed that understanding a threat to national security can take years. It is not the case that all threats are readily apparent

---

6 These operations are authorized by a Federal Court judge under s. 21 of the *CSIS Act*. See Chapter IV for further discussion of these search powers.

7 R.S.C. 1985, c. C-23.

or that their danger is immediately understood. Accordingly, CSIS conducts many long-term investigations that require patience and careful analysis of a large amount of intelligence. CSIS has an incentive to maximize secrecy and to continue its covert intelligence investigation to maximize its understanding of the threat. At the same time, it may not always serve the public interest to keep secret the intelligence that CSIS collects.

When should the intelligence collected by CSIS be passed on to the RCMP? When a dispute arises, it should be up to the NSA to make this decision.

2.2.1 Inherent Tensions between CSIS and the RCMP

Conflict between CSIS and the RCMP stems from their core mandates. CSIS is an intelligence agency that relies on secret sources and information received in confidence from allies to inform the Government of Canada about threats to the security of Canada. In contrast, the RCMP is a police force dedicated to collecting evidence of crimes for public prosecutions.

At present, to manage the information flow between them, the two agencies are left to devise non-statutory and non-binding mechanisms which do not interfere with their very different functions. The success of these mechanisms turns largely on the personalities of the employees in the two agencies. Although relations continue to improve, there remains a lack of understanding on the part of each agency of the other's functions and national security mandates.

CSIS has at least three concerns that adversely affect relations with the RCMP:

- Experience has shown that when the CSIS shares information with the RCMP, the RCMP has failed to respect the intelligence mandate by endangering sources, disclosing allies' confidences and making investigations by CSIS much more difficult;
- CSIS is alarmed by the scope of *Stinchcombe*[8] disclosure obligations, which create a risk of public exposure of intelligence operations and reduce the effectiveness of CSIS; and
- CSIS fears that closer cooperation will blur the lines between a civilian intelligence function and a law enforcement function. Put bluntly, CSIS fears that this would render it a substitute police force or that police will increasingly intrude into civilian intelligence matters.

For its part, the RCMP has chosen to manage the relationship with CSIS by treating CSIS as a "tip service." By applying a philosophy of "the less information we obtain from CSIS, the better," the RCMP hopes to lessen the chances of a conflict with CSIS and increase the likelihood of a successful police investigation. The RCMP has at least three concerns that adversely affect relations with CSIS:

---

8 *R. v. Stinchcombe,* [1991] 3 S.C.R. 326.

- The RCMP doubts whether CSIS appreciates the overlap of their mandates in counterterrorism matters. As a result, there is a perception that CSIS has an unsophisticated understanding of its impact on criminal investigations;
- The RCMP fears that CSIS has disregarded evidentiary standards about the collection and retention of intelligence; and
- The RCMP is concerned that CSIS will seek to protect its own investigations in preference to criminal investigations.

The RCMP's "the less information we obtain from CSIS, the better" approach to involvement with CSIS increases the potential for duplication and conflict. As will be discussed below, the two agencies have employed a rather elaborate process to avoid this. That process does not mean integration or cooperation. Most often, it emphasizes a separation of activities that enables each agency to stay out of the other's way.

2.2.2 Joint Management Team Meetings

The RCMP and CSIS have regular meetings at both the regional and headquarters levels where the agencies review their respective case inventories to ensure that there are no conflicts arising during their respective investigations and to address any conflicts that do arise. In essence, the RCMP discloses to CSIS all the targets of RCMP investigations and may provide a brief synopsis of the status of each investigation. CSIS attempts to review the material and indicates where there is a conflict. If there is a conflict, the agencies negotiate how to manage it.

RCMP Superintendent Jamie Jagoe[9] testified that, in resolving conflicts, he does not tell CSIS what to do, nor does CSIS direct the RCMP. Instead, a cooperative approach is taken to ensure respect for each other's mandate while each continues with its investigation.[10]

For example, if the RCMP is conducting an investigation into a matter that is also being monitored by CSIS, CSIS may chose to take a more passive role to permit the RCMP to acquire the evidence to build its case. As well, this process allows CSIS to remove human sources that are within a group targeted by the RCMP to avoid public exposure of these sources if a police investigation leads to a prosecution, thereby preserving the integrity of the CSIS investigation.

If a conflict between CSIS and the RCMP cannot be resolved at the regional level, the matter is dealt with at the headquarters level. Almost all witnesses thought it extremely unlikely that matters could not be worked out at the regional level. As well, given the extent of ongoing dialogue between the two agencies, there

---

9 RCMP Superintendent, Assistant CROPS Officer for National Security for O Division (which is the Province of Ontario).

10 Testimony of Jamie Jagoe, vol. 82, November 23, 2007, p. 10460.

should not be any surprises when reviewing each other's targets. Nevertheless, witnesses acknowledged that, if an irreconcilable difference arose between CSIS and the RCMP, the matter could end up before the Minister of Public Safety, who has ministerial responsibility for both agencies.

The agencies appear to be making a concerted effort to understand the scope of the other's investigations to ensure that they do not compromise each other's efforts. This process is an important and necessary part of the relationship between the RCMP and CSIS. However, these meetings, and this process for avoiding conflicts, do not address the fundamental problem of how to manage the transition from an intelligence investigation to a police investigation.

At the headquarters level, CSIS and the RCMP have regular Joint Management Team (JMT) meetings. The purpose of the JMT is to identify areas of concern to the two agencies and to determine how best to manage resources from their headquarters' perspectives. There is sensitivity to the fact that front line officers have to resolve many of these issues. Nevertheless, the officials at the headquarters level can provide guidance and a broader perspective than is available in the regions. CSIS can also use the JMT to inform the RCMP about new threats. However, CSIS will not always wait until a JMT meeting to discuss an issue. As RCMP Assistant Commissioner Mike McDonell remarked, "The regularized forum would be the Joint Management Team but in a lot of instances, we speak to the matter as the matter arises; we don't wait for the JMT. So the whole trick is not to impede or impair the investigators and to facilitate the work on the front line. So it's been my experience that we pick up the phone or go to one another's offices and deal with it forthwith."[11]

While there is some discussion between CSIS and the RCMP about alternatives to using law enforcement, the reality is that the default course of action is to commence a police investigation. Typically, the only issue is timing – when the RCMP should commence its investigation. McDonell noted that "…[i]t's much easier for [CSIS] to harvest from us or from our actions than for us to harvest from the Service's action. So that if we're looking at a specific event where there must be an intervention, it's much easier in the long run if the Royal Canadian Mounted Police conduct the inquiries, conduct the search or do whatever is required and the Service can have access to the fruit of our labour. But our primary purpose is to collect evidence and the reverse is a little more difficult. So it's been my experience in this job that we've always defaulted to the RCMP conducting the primary action."[12]

McDonell's comments exemplify the approach of "the less information we obtain from CSIS, the better." This suggests that the RCMP is generally not receiving all the intelligence from CSIS that it could.[13]

---

11 Testimony of Mike McDonell, vol. 95, December 13, 2007, p. 12654.

12 Testimony of Mike McDonell, vol. 95, December 13, 2007, p. 12637.

13 Means to improve the protections of intelligence from disclosure, while still preserving the accused's right to a fair trial, are discussed in Chapters V-VII. These chapters examine disclosure standards, privileges and the means to obtain judicial non-disclosure orders in specific cases.

As well, McDonell's evidence suggests that, instead of CSIS supplying the RCMP with detailed intelligence about possible terrorist threats, the RCMP is providing intelligence to CSIS. There are obvious benefits to the RCMP sharing information with the CSIS with respect to their often overlapping counterterrorism investigations.[14]

CSIS alone controls the quality, volume and timing of disclosure to the RCMP. Section 19(2)(a)[15] of the *CSIS Act* gives CSIS discretion to decide whether to share relevant intelligence with the police.[16]

Once intelligence is provided to the police, there is a risk that criminal investigations and prosecutions may be commenced, even though this may not be the most effective way to manage the terrorist threat. The JMT is not institutionally equipped to assess management strategies other than the use of law enforcement. The JMT is narrow in its focus in that the choice is typically between maintaining the CSIS investigation and turning the matter over to the RCMP. The JMT is not the place for strategic decision- making about the appropriate response to a particular security threat or even for strategic decision-making about whether a terrorism prosecution is in the public interest.

A further disadvantage of relying on the JMT as the locus for managing terrorist threats is the risk of public exposure of CSIS information that has been provided at JMT meetings. Although section 38 of the *Canada Evidence Act*[17] may provide protection for information disclosed to the JMT, the presence of the police imports the full menu of constitutional protections, including rights to disclosure of information, that are afforded persons who are the subject of criminal investigations. The risk of public disclosure of information from a police investigation should be accepted only after careful consideration. As discussed below, the NSA, with full input from all affected agencies, would be in the best position to determine if disclosing secret intelligence is in the public interest.

---

14 Stanley Cohen has argued that "the generous sharing 'up' of information and data from law enforcement to security intelligence is to be encouraged, provided, of course, that adequate safeguards, oversight and monitoring are features of the system as a whole": Stanley A. Cohen, *Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril* (Markham: LexisNexis, 2005), p. 406 [Cohen, *Privacy, Crime and Terror*].

15 Chapter IV discusses reforms to s. 19 to ensure that CSIS is required to share relevant intelligence directly with the police or the National Security Advisor and that it no longer have the discretion that it currently exercises to withhold relevant intelligence.

16 Stanley Cohen notes that s. 19 of the *CSIS Act* "provides an express grant of authority to the Canadian Security Intelligence Service to disclose information that it has lawfully obtained to law enforcement": Cohen, *Privacy, Crime and Terror*, p. 407. He further notes that the discretion of CSIS to share such information is influenced by a variety of factors including "the fact that the disclosure of subject information may ultimately become public in an open proceeding, such as a criminal trial; the downstream implications of revealing information that may ultimately tend to reveal covert, secret or surreptitious operational practices and techniques; the need to protect sensitive sources; and the requirement to adhere to agreements and undertakings with other nations in the interest of securing the nation's security and of promoting international cooperation and comity with Canada's friends and allies in the international community": p. 408.

17 R.S.C. 1985, c. C-5.

2.3 The Current Role of the National Security Advisor

In late 2003, a National Security Advisor to the Prime Minister was appointed "… to improve coordination and integration of security efforts among government departments."[18] This was a positive and necessary development, given the difficulties in cooperation and coordination among various agencies during both the pre- and post-bombing phases of the Air India investigation.

Due to the importance of coordinating national security activities, several witnesses from within and outside government were asked to comment on the role of the NSA when they appeared before the Commission.

The NSA is one of the most senior officials in the Privy Council Office (PCO). The PCO serves as a secretariat to ensure the smooth functioning of Cabinet. It is also the Prime Minister's "…source of public service advice across the entire spectrum of policy questions and operational issues facing the Government."[19] It is headed by the Clerk of the Privy Council who is the Prime Minister's Deputy Minister.[20]

The NSA has several roles:

- as Associate Secretary to the Cabinet, who acts "…on the Clerk's behalf on any of the policy and operational issues that come before the Privy Council Office;"[21]
- as NSA, who "…ensures the effective coordination of Canada's security and intelligence community;"[22]
- as Deputy Minister for Operations and Policy for the Communications Security Establishment (CSE); and
- as NSA, to oversee "…the provision of intelligence assessments to the Prime Minister, other ministers and senior government officials."[23]

Former NSA William Elliott, who is currently the Commissioner of the RCMP, told the Commission that one of his important duties was to play "a very central

---

18 Canada, *Securing an Open Society: Canada's National Security Policy* (April 2004), p. 9, online: Government of Canada Depository Services Program <http://dsp-psd.pwgsc.gc.ca/Collection/CP22-77-2004E.pdf> (accessed June 4, 2009) [*Canada's National Security Policy*].

19 Privy Council Office, "The Role and Structure of the Privy Council Office 2008," 1.0, online: Privy Council Office <http://www.pco-bcp.gc.ca/index.asp?lang=eng&page=information&sub=publications&doc=Role/role2008_e.htm#1> (accessed July 29, 2009).

20 Privy Council Office, "The Role and Structure of the Privy Council Office 2008," 2.0, online: Privy Council Office <http://www.pco-bcp.gc.ca/index.asp?lang=eng&page=information&sub=publications&doc=Role/role2008_e.htm#2> (accessed July 29, 2009).

21 Privy Council Office, "The Role and Structure of the Privy Council Office 2008," 3.0, online: Privy Council Office <http://www.pco-bcp.gc.ca/index.asp?lang=eng&page=information&sub=publications&doc=Role/role2008_e.htm#3> (accessed July 29, 2009) ["The Role and Structure of the Privy Council Office 2008," 3.0].

22 "The Role and Structure of the Privy Council Office 2008," 3.0.

23 "The Role and Structure of the Privy Council Office 2008," 3.0.

role" with respect to the work of the Cabinet committee responsible for national security. Part of his role involved "…coordination efforts, including work done by and in support of ministers on that committee." He also testified that the NSA plays an important role "…with respect to getting people from interested departments and agencies together to deal with important matters relating to national security including where there were fairly significant, at least at the beginning, differences of views with respect to things…." He said that what he had specifically in mind was work in relation to the application of section 38 of the *Canada Evidence Act* and the experience gained in dealing with issues relating to the O'Connor Inquiry. There, he said, "…the National Security Advisor certainly played a role with respect to the development of a government position which resulted in a position of the government as decided and articulated by ministers."[24]

The NSA at the time of the Commission hearings, Margaret Bloodworth, described her position as consisting of three roles: an advisory role, a coordination role and an operational role with CSE. She acts as an advisor to the Prime Minister and to a Cabinet committee on intelligence programs and national security policies. The NSA also acts as the Associate Secretary of the Cabinet. Bloodworth also spent time on public service renewal at large, particularly relating to the intelligence community.

Bloodworth described her coordination role as "…co-ordinating with regard to intelligence, to carry things like development of priorities and overall assessment. And secondly, on national security more generally which would include response and resilience and border issues…."[25] She added that her coordination role with respect to the RCMP and CSIS would be exercised without interfering with the ultimate responsibility of the Minister of Public Safety for both agencies, which she described as "…pretty fundamental to our system."[26]

Nevertheless, she noted, the NSA's coordination role could include meeting with the heads of RCMP and CSIS and saying, "…'[y]ou two should fix this' or some variation thereof or perhaps Justice could play a role if it was a legal issue and so on. If in the end it was not resolvable, then it would be up to their minister to take action and if they didn't bring it to their minister I would feel some onus to make sure their minister was aware of it. Now, I don't think it would come to that because there's also a Deputy Minister of Public Safety who would know something about that."[27]

The NSA also chairs a committee of deputy ministers on national security that meets roughly once a month or every six weeks and considers "a whole range" of national security issues, including "lessons learned."[28]

---

24 Testimony of William Elliott, vol. 90, December 6, 2007, p. 11827.
25 Testimony of Margaret Bloodworth, vol. 95, December 13, 2007, pp. 12671-12672.
26 Testimony of Margaret Bloodworth, vol. 95, December 13, 2007, p. 12676.
27 Testimony of Margaret Bloodworth, vol. 95, December 13, 2007, pp. 12676-12677.
28 Testimony of Margaret Bloodworth, vol. 95, December 13, 2007, pp. 12681-12682.

Finally, the NSA is also the Deputy Minister for Operations and Policy for the CSE. In that capacity, Bloodworth becomes involved in the operations of CSE, especially as they relate to the Government of Canada's intelligence priorities and other security agencies.[29] The CSE has a three-part mandate under the *National Defence Act*:

- to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence in accordance with the Government of Canada's intelligence priorities;
- to provide advice, guidance and services to help protect the Government's information infrastructures; and
- to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.[30]

In short, the NSA has multiple policy, coordination and operational responsibilities.

The NSA is assisted by a Deputy National Security Advisor and by two secretariats within the PCO: the Security and Intelligence Secretariat and the International Assessment Staff Secretariat. The Security and Intelligence Secretariat works with federal departments to coordinate a range of security measures. These include the security component of the Security and Prosperity Partnership of North America and issues relating to the security of the Prime Minister, the Cabinet, the Government and the National Capital Region. The International Assessment Staff Secretariat provides information relating to terrorism through the Integrated Threat Assessment Centre (ITAC) and directly from Canada's allies. The Executive Director of the International Assessment Staff Secretariat and the Assistant Secretary to the Cabinet (Security and Intelligence) both report to the NSA through the Foreign and Defence Policy Advisor to the Prime Minister. Both the NSA and the Foreign and Defence Policy Advisor support the Cabinet Committee for Foreign Affairs and National Security.[31]

2.3.1 Competing Views on the Adequacy of the Coordination Powers of the National Security Advisor

Professor Martin Rudner, Distinguished Research Professor Emeritus at the Norman Paterson School of International Affairs at Carleton University, saw the present function of the NSA as "…to advise the Prime Minister on national security; it is manifestly not to coordinate the security intelligence community. There are no resources, instruments or intent."[32] He also rejected the idea that

---

29 Testimony of Margaret Bloodworth, vol. 95, December 13, 2007, pp. 12671-12672.
30 R.S.C. 1985, c. N-5, s. 273.64.
31 Privy Council Office, "The Role and Structure of the Privy Council Office 2008," 8.0, online: Privy Council Office <http://www.pco-bcp.gc.ca/index.asp?lang=eng&page=information&sub=publications&doc=Role/role2008_e.htm#8> (accessed July 29, 2009).
32 Testimony of Martin Rudner, vol. 92, December 10, 2007, pp. 12254-12255.

the Department of Public Safety could play a coordinating role, stating that "… it's a big bill for a young department."[33] In a paper prepared for the Commission, Rudner proposed a significant enhancement of the role of the NSA to include the resources to make supplementary budgetary appropriations and additional personnel allocations and to use moral suasion.[34] Rudner argued that a proactive "whole of government," intelligence-led approach required "…a significant enhancement of this coordination function in order to ensure policy coherence, inter-agency cooperation, and effective synergy among a wide array of security, intelligence and law enforcement organizations, relevant governmental departments (at all levels), and even private owner/operators of critical national infrastructure."[35]

Professor Bruce Hoffman, of the Edmund Walsh School of Foreign Service at Georgetown University, testified that the essential powers of an intelligence coordinator consisted of the ability to set standards across the intelligence community, budgetary control and personnel control. A person in charge of coordinating and overseeing the intelligence community "…required control over the purse strings, that is budgetary control; the ability to hire and fire senior managers and then the ability to set standards for both the information structure and personnel across the entire intelligence community."[36] In his view:

> "[T]he magnitude of the threat and the complexity of the threats that's posed to our countries in the 21st century means that you have to have an individual that again can reach across the stakeholders, set the priorities, because these priorities are not the priorities of individual agencies; we're talking about national priorities, and then, having set the priorities, to actually dictate the tasking. I think this is enormously important. Not just to sometimes force reluctant bureaucracies out of their comfort zone or out of their box, but also to provide the strategic dimension to ensure that the focus is on precisely those priorities that are most critical to national security."[37]

Rudner and Hoffman were not alone in arguing that there was a need for enhanced coordination powers in national security matters. Norman Inkster, a former Commissioner of the RCMP, agreed with the suggestion that there is a need for an arbiter to decide disputes between CSIS and the RCMP about the handling of sources.[38]

---

33 Testimony of Martin Rudner, vol. 92, December 10, 2007, pp. 12257-12258.
34 Martin Rudner, "Building Canada's Counter-Terrorism Capacity: A Proactive All-Of-Government Approach to Intelligence-Led Counter-Terrorism" in Vol. 1 of Research Studies: Threat Assessment RCMP/CSIS Co-operation, pp. 137-139 [Rudner Paper on Building Counter-Terrorism Capacity].
35 Rudner Paper on Building Counter-Terrorism Capacity, p. 138.
36 Testimony of Bruce Hoffman, vol. 94, December 12, 2007, p. 12530.
37 Testimony of Bruce Hoffman, vol. 94, December 12, 2007, p. 12514.
38 Testimony of Norman Inkster, vol. 81, November 22, 2007, p. 10368.

Giuliano Zaccardelli, also a former Commissioner of the RCMP, testified that a change of governance was required to stop the practice of agencies operating in silos, exchanging information only on an *ad hoc* basis. He called for a governance body, staffed by officials from the highest levels of the key intelligence agencies, that would be responsible for ensuring the safety and security of Canada. The governance body would be able to make resources available and integrate them in a way that would ensure that "…the whole is greater than the sum of its parts."[39] Zaccardelli argued that the work of the governance body should be facilitated by someone outside of government.[40] He did not think that this role should be filled by a minister, because of the risk of political interference, or by a senior bureaucrat, because of the risk of being captured by "vested interests."[41] Rather, the person should have the credibility and stature to bring the various agencies together "…and make them work for the good of Canada."[42]

Reid Morden, a former Director of CSIS, testified that there was not enough "… clout within the current structure to bring about the coordination and to give direction to this rather multi-headed intelligence beast which we have created." He testified that the coordinator should not be in the Prime Minister's Office, but that the person "…should have direct access to the Prime Minister who has always, at least in title, chaired any Cabinet committee which has dealt with security or intelligence affairs."[43] He testified that there was a need for "…a new look at the kind of machinery we have," as governments responded "…to a world which has become a much more dangerous and a much more ruthless place than it was a number of years ago."[44]

Not all witnesses agreed that the NSA needed greater coordination powers. The Hon. Ronald ("Ron") Atkey, the former chair of SIRC and a person with extensive experience in national security matters, testified that Canada was "…not mature enough yet to go for a security czar. We see attempts in the United States now to move in that direction, but they are still having difficulties…."[45]

Former NSA Elliott testified that he was not sure that creating a new entity, "… whether…called an 'Intelligence Czar' or some other thing, is really necessary or desirable. If it was – if a principal objective was to resolve disputes, I don't think the individual would be very busy and…I'm not sure of the merits of putting somebody in charge of operations across government departments and agencies. I'm not sure that that would lead to very effective operations, frankly."[46]

---

39 Testimony of Giuliano Zaccardelli, vol. 86, November 30, 2007, pp. 11030-11032.
40 Testimony of Giuliano Zaccardelli, vol. 86, November 30, 2007, p. 11077.
41 Testimony of Giuliano Zaccardelli, vol. 86, November 30, 2007, pp. 11080-11081.
42 Testimony of Giuliano Zaccardelli, vol. 86, November 30, 2007, p. 11078.
43 Testimony of Reid Morden, vol. 88, December 4, 2007, pp. 11455-11457.
44 Testimony of Reid Morden, vol. 88, December 4, 2007, p. 11456.
45 Testimony of Ronald Atkey, vol. 49, September 20, 2007, p. 6030.
46 Testimony of William Elliott, vol. 90, December 6, 2007, p. 11828.

Jim Judd, the Director of CSIS at the time of his testimony and who has since retired, also testified that there was no need for an enhanced coordination role in Canada. He stated that, "…[i]n our circumstances here in Canada, I think it's probably fair to say that in respect of anything that we do in our organization, internationally or domestically that is of note, in our view, the National Security Advisor and the Minister and very often Prime Minister know about it as it happens, so that I think we have perhaps a bit of a better history of ensuring that those communications channels do exist. And it's partly a functional fact that, of course, you're dealing with a much smaller universe in the Canadian context than you are in the United States. I don't know of any other Western jurisdiction other than the United States which has sought to impose this kind of regime of a super personality at the top of the system. And I don't, in current circumstances, certainly see the need for that to happen here, given the arrangements that already exist."[47]

Finally, Margaret Bloodworth, the NSA at the time of our hearings, argued that Professor Hoffman's proposals for increased coordination were not compatible with a parliamentary system where ministers are ultimately accountable for the performance and budgets of the agencies in their ministries. With respect to budgetary issues she saw difficulties in "…splitting money from accountability": "And I think accountability matters, and I'm actually a believer in Ministers, to the extent possible, being accountable at the end of it, and I think there's a limit to how much you can make the Prime Minister personally accountable."[48] She added that "…having run three different departments now, it's not been my experience that money managed from the centre is managed more effectively than [money] managed in departments." [49]

It could be argued that the Minister of Public Safety, rather than the NSA, should play a coordinating role for national security activities. At present, the Minister of Public Safety is responsible for the RCMP and CSIS. Both agencies at times seem to be more powerful than their Minister. This is because Public Safety, as a direct descendant of the former Ministry of the Solicitor General, may be seen as insufficiently senior within government to take the lead on complex national security matters.

There are limits to the jurisdiction of the Minister of Public Safety. While CSIS, CBSA and the RCMP fall within the Minister's jurisdiction, significant players such as DFAIT, DND and CSE do not. As well, the decision about how to manage a particular terror threat may very well engage our international strategic interests. DFAIT can and ought to make an important contribution in such cases. The Attorney General of Canada, who is outside the Department of Public Safety, also has important responsibilities for the approval of terrorism prosecutions and for the protection of secret information from disclosure.

---

47 Testimony of Jim Judd, vol. 90, December 6, 2007, pp. 11866-11867.
48 Testimony of Margaret Bloodworth, vol. 95, December 13, 2007, pp. 12684-12687.
49 Testimony of Margaret Bloodworth, vol. 95, December 13, 2007, p. 12689.

It is the Commission's view that national security is far too important to leave in the hands of one minister or agency. The Ministry of Public Safety does not command the national security apparatus. Only the Prime Minister's delegate can have the legitimacy to wield that power.

2.3.2 The Legitimate Role of the Prime Minister and the Privy Council Office in Coordinating National Security Activities

The need for the Prime Minister and the Privy Council Office to play a key role in national security matters has long been recognized. A 1969 Royal Commission on Security observed that, while the Privy Council Office provided some support to Cabinet committees on security and meetings of the relevant deputy ministers, the effectiveness of this central coordination was "…more apparent than real."[50] The Royal Commission recommended that a Security Secretariat within the Privy Council Office be given adequate authority, resources and staff "…to formulate security policy and procedures in the context of general governmental policies, and more importantly, with effective authority to supervise the implementation of government security policies and regulations and to ensure their consistent application."[51]

Although the security environment is very different today from that of 1969, the basic insight of that Commission still rings true: "…under present arrangements the total view of the requirements of security may often be obscured by the pressures exerted by individual departments."[52] Indeed, the danger of failing to see the "big picture" and of losing central oversight and control is even greater today, since many more agencies than before have security responsibilities in the post-9/11 environment.

The Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (McDonald Commission) recommended that the Prime Minister chair a Cabinet committee on security and intelligence because "…[w]eaknesses in the internal security system can have drastic consequences for the well-being of the nation. The secret, intrusive nature of security work makes it dangerous to permit any Minister to become overly dominant in this field. The consideration of intelligence needs should be a balanced process free from domination by any single government department."[53]

In his 2006 report, Commissioner O'Connor recognized that, "…[a]s the head of government in Canada, the Prime Minister has ultimate responsibility for national security."[54] In discharging these responsibilities, the Prime Minister is assisted by the Privy Council Office (PCO) which "…provides non-partisan advice

---

50 *Report of the Royal Commission on Security*, p. 17.
51 *Report of the Royal Commission on Security*, pp. 18, 105.
52 *Report of the Royal Commission on Security*, p. 17.
53 *Freedom and Security under the Law*, Second Report - vol. 2, p. 847.
54 *A New Review Mechanism for the RCMP's National Security Activities*, p. 196.

and support for the Prime Minister, departments within the Prime Minister's portfolio, the federal Cabinet and Cabinet committees."[55]

The natural locus for coordinating federal agencies involved in preventing and prosecuting terrorism is the Privy Council Office. This was recognized by the federal government when the position of Prime Minister's National Security Advisor was established in 2003.

The clear trend in this area has been to centralize operations as much as possible. For example, the RCMP has gone to great lengths to centralize terrorism investigations. CSIS has been highly centralized since its inception. Centralization of national security investigations is a virtual necessity, given that most, if not all, national security investigations have national and international aspects.

Centralization permits a broader approach to decision making and ultimately promotes cooperation between agencies. Without a centralized, cross-ministry rationalization of Canada's national security infrastructure, government will not address the long-term structural issues that have plagued the RCMP and CSIS. A failure to address these issues would leave Canadians relying solely on the goodwill of those who currently hold senior positions at those agencies.

Increased coordination is possible in the national security field because the Prime Minister is the first among equals and, with limited exceptions,[56] can take responsibility for decisions in the national security area. Fears that officials in the Privy Council Office will abuse their power, or not be held accountable for its exercise, overlook the fact that the Prime Minister is responsible for their conduct. The Prime Minister is also responsible and accountable to Parliament for the Government's overall performance in national security matters. The Prime Minister's special role in national security simply recognizes the reality that the Prime Minister has the ultimate decision-making authority in almost all national security matters.

Although she stressed the importance of ministerial accountability and responsibility in her testimony, Bloodworth recognized the reality of the Prime Minister's pre-eminent role when she testified that, even with respect to matters within the portfolio of the Minister of Public Safety, "…it's possible the Prime Minister might be brought in, then I provide advice there."[57] The roles of the Prime Minister and the PCO do not generally affect day-to-day operations, but rather involve setting national security policy and priorities, ensuring that the ministries and agencies implement the policy, and resolving high level disputes involving policy matters.

---

55 *A New Review Mechanism for the RCMP's National Security Activities*, p. 196.
56 The role of police and prosecutorial independence and discretion is discussed in Chapter III.
57 Testimony of Margaret Bloodworth, vol. 95, December 13, 2007, pp. 12679-12680.

The idea that, on national security matters, the ultimate authority in most matters rests with the Prime Minister accords with Canada's democratic traditions. It also accords with the commonsensical expectations of Canadians.

It is important that the Prime Minister receive expert advice from senior civil servants in the Privy Council Office. The suggestion that an enhanced national security coordination role in the PCO would be too "political" should be rejected. As Elliott testified, "Canada has a long, important, proud history of independence of the public service." Furthermore, "…when governments change as they frequently do at least in the modern context, there is not a wholesale or immediate change of senior officials, and just as I was the National Security Advisor to Prime Minister Martin, I was the National Security Advisor to Prime Minister Harper and my roles and relationships with the Prime Minister and the Prime Minister's Office really didn't change substantially because one government went out of office and another government came into office."[58]

Although ministers should, by law and tradition, remain accountable for their departments and for the agencies in those departments, it is the Prime Minister, assisted by experts in the Privy Council Office, who can assess the security needs of the Government and assess the public interest in determining the appropriate response to a given threat.

In summary, the Prime Minister and the Privy Council Office have vital and legitimate roles to play in national security matters. These roles include:

- establishing strategic national security policies and priorities;
- coordinating national security activities, including the distribution of intelligence;
- resolving disputes between the agencies and ministries that have national security responsibilities; and
- overseeing the effectiveness of national security activities.

The exercise of these important roles is in keeping with Canada's tradition of parliamentary democracy and with the role of the Privy Council Office in providing impartial and non-partisan public service advice and expertise to the Prime Minister.

2.3.3 Expanding the Role of the National Security Advisor

At present, the NSA's mandate is ill-defined. This mandate should be enhanced and clarified. The nature of Canada's multi-faceted national security activities and the challenging task of establishing priorities for these agencies, coordinating them, resolving disputes among them and determining whether they are working together effectively will require a substantial enhancement of the NSA's role.

---

58 Testimony of William Elliott, vol. 90, December 6, 2007, pp. 11828-11829.

An enhanced mandate for the NSA is especially necessary to better balance the pressure to keep intelligence secret with the conflicting pressure to allow it to be used as evidence. In addition, the NSA needs greater powers to oversee the effectiveness of the agencies and departments responsible for national security activities.

An NSA with enhanced responsibilities should at a minimum continue to hold the NSA's current rank as the National Security Advisor and Associate Secretary to the Cabinet, just below the Clerk of the Privy Council and Secretary to the Cabinet.[59]

2.3.3.1 Establishing Strategic National Security Policies and Priorities

In 2004, Canada established its first official National Security Policy.[60] An official policy was necessary because of the changed threat environment and because so many parts of the government now exercised national security responsibilities – ranging from the collection of intelligence to the discharge of responsibilities for emergency preparedness and management. The national security policy devoted a whole chapter to "…building an integrated security system" in recognition that "…the lack of integration in our current system is a key gap…."[61] It proposed an integrated security system that would include threat assessment, protection and prevention, evaluation and oversight, and consequence management.[62] The policy recognized that "…[a]n effective national security framework must, of necessity, be a continual work in progress. We need to continuously evaluate the success of the system by testing its effectiveness."[63]

The National Security Policy stressed the need for more coordination and strategic planning for a wide array of security initiatives, including transportation safety, intelligence and international security. To implement this security policy, or any other that the Government may develop, it will be necessary to have a broad vision of government's abilities and responsibilities.

A chapter in the 2004 National Security Policy was devoted to intelligence. Security intelligence agencies are deliberately subject to fuller political direction than police and prosecutors. In Canada's system, the responsible minister is accountable for these agencies but, as suggested earlier, the Prime Minister and his advisors have a pre-eminent role in establishing priorities and policies in the national security field. There is a need to ensure that the priorities of security intelligence agencies reflect the best strategic judgments of the Government of

---

59 Privy Council Office Organization Chart (March 2009), online: Privy Council Office <http://www.pco-bcp.gc.ca/docs/Org/2009-03-eng.pdf> (accessed June 4, 2009).

60 Canada, *Securing an Open Society: Canada's National Security Policy* (April 2004), online: Government of Canada Depository Services Program <http://dsp-psd.pwgsc.gc.ca/Collection/CP22-77-2004E.pdf> (accessed June 4, 2009) [*Canada's National Security Policy*].

61 *Canada's National Security Policy*, p. 9.

62 *Canada's National Security Policy*, pp. 10-13.

63 *Canada's National Security Policy*, p. 12.

Canada. As Professor Hoffman suggested, a critical responsibility of an NSA is to establish community-wide intelligence priorities.[64]

Intelligence priorities should be centrally coordinated, informed by careful analysis of intelligence to determine the most important threats, the biggest gaps and the most strategic vulnerabilities.[65] This does not mean that the Prime Minister or the NSA should run CSIS or the CSE. These agencies will develop their own strategic plans, consistent with the priorities set by the Government of Canada. In appropriate cases, however, it is perfectly permissible for the Government, acting through the Prime Minister and the NSA and in consultation with the appropriate minister(s), to adjust the priorities of intelligence agencies and to coordinate them with other Government priorities.

The setting of priorities in the national security field is a matter of daunting complexity. There is a need for input from many departments and agencies, and Canada's National Security Policy can be influenced by a wide range of domestic and international factors. Only the Prime Minister and the NSA can ensure that each agency's priorities fit into the larger picture. Only they have the incentive and the ability to determine if the multiple departments and agencies with national security responsibilities are working well together.

As discussed earlier, the NSA already has responsibilities as a Deputy Minister for the Communications Security Establishment, Canada's signals intelligence agency, which obtains information from the global communications infrastructure. Although this responsibility may be delegated to the Deputy National Security Advisor because of the enhanced responsibilities that would be given to the NSA under the Commission's recommendations, it is important that the NSA retain some connections with CSE. As the narrative of this report has revealed, relevant information obtained by CSE was not distributed before the Air India bombing. Increases in the threat of international terrorism make it more likely that CSE will obtain information of relevance to the NSA and other agencies. It is also important that the activities of CSE be guided by the Government's intelligence priorities.

The establishment of priorities is a critical function of the NSA. This function cannot be carried out without adequate staff. As suggested by Rudner, the establishment of national security priorities should ideally be informed by intelligence analysis. The talent for such analysis is most likely to be found within the intelligence agencies, but, as Rudner suggests, there is a need to ensure better career paths for such analysts, which may include time in the PCO.

As national security activities expand into areas such as aviation security and preventing terrorist financing, there is a greater need to establish strategic policies and priorities. Although the responsible agencies and departments should develop policies in the first instance, the NSA might have a role in

---

64 Testimony of Bruce Hoffman, vol. 94, December 12, 2007, pp. 12544-12545.
65 Rudner Paper on Building Counter-Terrorism Capacity, pp. 133-137.

ensuring that the policies accord with overall governmental policies. The NSA might also help resolve disputes about the nature of a particular policy or its implementation.

The NSA might also play a role in developing policy to respond to deficiencies in anti-terrorist-financing programs, which may be revealed by domestic or international reviews or by conflicts between the multiple agencies that are involved in preventing terrorist financing. One example is the need to establish adequate performance indicators and assessment mechanisms for programs aimed at terrorist financing. Although the NSA would call on the agencies to implement the policies, the NSA would have a role in ensuring that adequate policies were in place and were followed.

2.3.3.2 Coordination of National Security Activities, Including Distribution of Intelligence

The NSA's present role should be expanded to include responsibility for the strategic coordination of the government's response to terrorist threats. The most important enhanced role might be to ensure coordination of the various agencies responsible for national security, including addressing issues that arise from the distribution of intelligence within government. The NSA might play an important role in ensuring that sufficient information is shared among agencies.

There is a need to ensure that intelligence gets into the hands of the proper decision makers. Such distribution should help prevent the dysfunctional relationships and poor flow of intelligence that tainted the pre- and post-bombing Air India investigations. There is also a need to ensure that intelligence agencies implement the priorities that have been set for them. At the same time, care should be taken to avoid collecting intelligence for the sake of collecting intelligence; the collection must have a legitimate purpose.

Unlike the Director of CSIS or the RCMP, the NSA should have no institutional bias favouring a particular response. The NSA should not have a bias towards maintaining the CSIS intelligence investigation or commencing a process that may end in a prosecution. Instead, the NSA should have the necessary independence to make decisions in the public interest regardless of their popularity with a particular agency.

The enhanced role of the NSA will require the NSA to work closely with the responsible ministers and deputy ministers to ensure compliance with the Government's national security strategy. For instance, in the unlikely event of a senior official rejecting specific advice from the NSA, that senior official would be required to provide a written explanation to the official's responsible minister. At that point, the matter would be dealt with at the ministerial level, with the involvement of the Prime Minister if needed.

In appropriate cases, ministers should intervene, as the former Solicitor General did to resolve the dispute between the RCMP and CSIS about access to CSIS material in the post-bombing Air India investigation. In such a case, the NSA can ensure that the Prime Minister is aware of, and supports, the minister's actions. The NSA may have an even more important role where two agencies headed by different ministers are not cooperating adequately. Examples could include conflicts between foreign affairs and domestic security agencies or conflicts involving the agencies responsible for anti-terrorist financing initiatives and aviation security.[66] The NSA would have the responsibility to manage interagency relationships so that conflicts are dealt with efficiently and in the public interest.

It is important that the NSA regularly brief the Prime Minister about threats to national security so that the Prime Minister can advise Cabinet colleagues. These briefings can assist the Prime Minister in dealing directly with the responsible ministers to ensure cooperation among agencies.

Each agency with national security responsibilities should have to submit to the NSA's decisions and authority. The only exception would be if the minister responsible for the agency was prepared to take the matter to the Prime Minister for decision. It is unacceptable for individual agencies to operate in silos, unconcerned about the impact of their decisions on other governmental actors or on the broader public interest.[67] Interagency competition must be avoided and strongly discouraged.

In difficult or disputed cases, the NSA would be responsible for determining how and when the government should respond. This might involve engaging the RCMP or Citizenship and Immigration, CBSA or CRA officials, or pursuing diplomatic initiatives. The NSA should determine, in his or her view, the most effective response in the public interest. The fact that the NSA reports directly to the Prime Minister will vest the position with sufficient power to command the respect of the agencies involved.

2.3.3.3 The Need for a Privilege to Protect the NSA's Deliberations and Information Received by the NSA

The ability of the NSA to perform this enhanced role will depend on the NSA's ability to obtain information from agencies with national security responsibilities. If CSIS provides information to the NSA, it will be necessary to ensure that this does not place the information at risk of public exposure. The advice and information provided to the NSA should be protected by a new national security

---

66 On the tensions between the role of Transport Canada and the Canadian Air Transport Security Authority (CATSA), see the review of the *Canadian Air Transport Security Authority Act* by the CATSA Advisory Panel: *Flight Plan: Managing the Risks in Aviation Security - Report of the Advisory Panel*, paras. 2.4 and 4.3 and ch.6, online: Transport Canada <http://www.tc.gc.ca/tcss/catsa/final_report-rapport_final/final_report_e.pdf> (accessed July 31, 2009).

67 There are some legitimate exceptions, given the constitutional status of police independence and prosecutorial discretion, both of which are discussed in Chapter III.

privilege, beyond the reach of the courts or access to information legislation. Similarly, the NSA's deliberations about managing terrorist threats should be privileged. This legal protection will construct a "safe house" in which CSIS, other agencies and the NSA can discuss a terrorist threat freely without concern that public exposure may thwart efforts to control the threat. Such a privileged "safe house" is necessary to ensure that the NSA can effectively coordinate the Government's response to security threats. The legal details of such a new privilege are discussed in Chapter VI.

The deliberations of the NSA, and information prepared by the agencies for the NSA, should be protected from disclosure by a new class-based national security privilege patterned after the privilege that applies to Cabinet deliberations under section 39 of the *Canada Evidence Act*. Making communications between CSIS and the NSA privileged would eliminate the concerns of CSIS about disclosure. The same privilege would also apply if the CSE or other agencies provided information to the NSA. All information prepared for and considered by the NSA would be covered by the new privilege.[68]

The NSA would have the authority to disclose information to the RCMP or to other agencies, and the privilege would not apply to information once the NSA disclosed it.[69] This privilege would respond to the risk that the information could not otherwise be protected from disclosure in legal proceedings by existing privileges or by judicial non-disclosure orders under sections 37 and 38 of the *Canada Evidence Act*.

Even without a new national security privilege, the risk is low that information produced for and by the NSA would have to be disclosed publicly. If attempts were made to obtain disclosure, the Attorney General of Canada could use section 38 of the *Canada Evidence Act* to prevent the disclosure on the basis of the harm that disclosure would cause to national security. For this reason, the measures recommended in this chapter to enhance the role of the NSA should not be delayed until the enactment of legislation on the new national security privilege.

If CSIS wanted to withhold information from another agency, the NSA would have the authority to require CSIS to provide the information to that agency. The NSA would consider the interests of CSIS and might chose a way to manage the threat that did not place the CSIS information or a related CSIS investigation at risk.

This new arrangement for sharing information with the NSA should not preclude CSIS from exercising its discretion to provide information to the RCMP.[70] CSIS

---

68 The details of this new privilege, patterned after the provisions for the confidentiality of Cabinet confidences in s. 39 of the *Canada Evidence Act*, R.S.C. 1985, c. C-5 [*Canada Evidence Act*], are discussed in Chapter VI.

69 Other privileges, such as national security privilege under s. 38 of the *Canada Evidence Act* could, however, still be claimed. This is discussed in Chapter VI.

70 This information will also have to be passed to the NSA.

would continue to share information when it decided that it was appropriate to do so. There would be no need to go through the NSA when CSIS decides to disclose information to another agency.

2.3.3.4 The Relationship between the NSA and CSIS

At present, sections 12 and 19 of the *CSIS Act* permit CSIS to share intelligence with other agencies in a number of situations. For example, the Service may share information with the RCMP, local law enforcement agencies, the Minister of Foreign Affairs, the Minister of National Defence or any other Minister of the Crown or person in the federal public administration.[71] Reform of the role of the NSA should not affect this. CSIS should continue to be able to pass on relevant information to the police and other officials.

Typically, CSIS will have obtained as much intelligence about a threat as anyone else in government. However, the NSA might sometimes want additional information or wish to solicit additional points of view. To that end, the NSA should be empowered to meet with representatives from any government agency – be it the CRA, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)[72] or any other agency – to discuss the threat and, where necessary, to seek information. As well, the NSA could simply ask CSIS to obtain the additional information that the NSA was seeking.

As discussed above, information provided to the NSA and discussions with the NSA should be protected by a new national security privilege. This will remove any incentive for agencies to withhold information from the NSA.

2.3.3.5 The Relationship between the NSA and Law Enforcement Agencies

The NSA is primarily concerned with responses to terrorist threats on the basis of intelligence information and has no responsibility for conducting criminal investigations. The NSA can provide information to the RCMP, which may lead it to commence a criminal investigation. However, once the information is passed to the RCMP, the NSA has no ongoing role in the investigation. It is a police matter.[73] The RCMP is then duty bound to conduct the investigation independent of any outside influence. At the same time, as will be discussed below, the NSA should be able to have contact with the RCMP about policy, dispute resolution or about general matters relating to the effectiveness of operations, particularly as they involve the RCMP working with other agencies. The NSA would have no direct relationship with municipal and provincial forces. These police forces already have various mechanisms to liaise with the RCMP.

---

71 *CSIS Act*, ss. 12, 19(2).

72 Limits placed on the disclosure of information from FINTRAC are discussed in Volume V. The NSA should not generally need access to such information for his or her coordination or dispute resolution duties. If necessary, the NSA could request CSIS or the RCMP to apply under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, S.C. 2000, c. 17 to obtain the necessary information.

73 Police independence is discussed in Chapter III.

This approach emphasizes the RCMP's independent and primary role as the police force responsible for criminal investigations relating to terrorism.

In some cases, it may be appropriate for the NSA to provide information to the Attorney General of Canada when that information is relevant to the exercise of prosecutorial discretion.[74]

In practice, Integrated National Security Enforcement Teams (INSETs) serve as information hubs for local police forces and CSIS. The basic principle is that local police forces move information that may have national security implications from local detachments to an INSET. The INSET, in turn, should send that information to CSIS to help CSIS generate intelligence. When CSIS provides advice to the NSA, CSIS will have benefited from any local police information in preparing that advice. The importance of the information flow from INSETs to CSIS and to the NSA will increase if domestic terrorist groups continue to develop as a serious threat to national security. CSIS will have sufficient coverage to understand a threat, but local police officers and others might provide useful additional sources of information for CSIS.[75]

2.3.3.6 Resolving Disputes between the Agencies, Including Disputes Arising from the Intelligence/Evidence Relationship

The NSA should also assist in resolving the disputes that will inevitably arise when multiple agencies with different mandates work on the same terrorist issues. Disputes will occur as a result of the competing demands, on one hand, to keep intelligence secret and, on the other, to disclose it for criminal trials. These conflicts cannot easily be resolved. All agencies involved could benefit from the NSA's participation. This is an area of critical importance, as revealed by the Air India investigation, and an area where Canada has the potential to break new ground in coordinating national security activities.

Conflicts may increase because many activities are newly described as terrorist crimes under the *Anti-terrorism Act,*[76] and because the nature of a terrorist threat may require law enforcement powers to be used to stop suspects from engaging in lethal terrorist activities.

Elliott testified that the NSA has played a role in bringing others together to discuss important matters of national security. His own experience included preparing the response to the O'Connor Commission.[77] This experience suggests that there is a legitimate role for central coordination with respect to some of the issues arising from the relationship between intelligence and evidence, even though the ultimate responsibility for dealing with issues of privilege under section 38 lies with the Attorney General of Canada.

---

74 Prosecutorial discretion is discussed in Chapter III.

75 As well, local forces may provide information of a national security offence that may form the basis of an investigation by the INSET.

76 S.C. 2001, c. 41.

77 Testimony of William Elliott, vol. 90, December 6, 2007, p. 11827.

The dispute resolution role of the NSA could help to prevent the types of conflicts that infected and slowed the Air India investigation. Bloodworth explained how the NSA can resolve disputes through the exercise of moral suasion. She described her ability to meet with the heads of CSIS and the RCMP to encourage them to resolve disputes.

Hoffman emphasized the important dispute resolution role that a national security coordinator could play. He testified that there is an "…advantage of having someone with this kind of responsibility…[to] facilitate the successful resolution of these types of internal conflicts or disputes…[to] adjudicate between the different agencies, not ride roughshod over them but, nonetheless, the direct opposite of having one agency to slam the door in the face of another agency and [the national security coordinator] at least can provide some mechanism to ensure the flow of appropriate intelligence and necessary intelligence to whom and where and when it's most needed."[78]

2.3.3.7 Oversight of the Effectiveness of National Security Activities

As the account of the pre- and post-bombing Air India investigation illustrates, the prevention and prosecution of terrorism implicates many agencies. These include police, security intelligence, transportation and immigration agencies, to mention a few. In a 2004 report, the Auditor General of Canada remarked on the need for improved coordination on security issues that "cross agency boundaries," such as "…information systems, watch lists, and personnel screening."[79] Later that year, the Auditor General commented, with respect to terrorist financing, that there was a lack of "…effective procedures for resolving interdepartmental disputes and ensuring accountability for results. We found, as we had in our audit of the anti-terrorism measures of 2001, that the government did not have a management framework to direct complementary actions in separate agencies."[80]

The work of the O'Connor Commission and the Iacobucci Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin also underline how various elements of the Canadian government, including CSIS, the RCMP and the Department of Foreign Affairs, may become involved in complex international terrorism investigations. The O'Connor Commission listed 16 departments and agencies that the federal government identified as having "key" national security responsibilities.[81] That Commission recommended a new, integrated, independent and self-initiated

---

78 Testimony of Bruce Hoffman, vol. 94, December 12, 2007, pp. 12519-12520.

79 *Report of the Auditor General of Canada to the House of Commons*, March 2004, Chapter 3: "National Security in Canada - The 2001 Anti-Terrorism Initiative," para. 3.161, online: Office of the Auditor General of Canada <http://www.oag-bvg.gc.ca/internet/docs/20040303ce.pdf> (accessed June 4, 2009).

80 *Report of the Auditor General of Canada to the House of Commons*, November 2004, Chapter 2: "Implementation of the National Initiative to Combat Money Laundering," para. 2.27, online: Office of the Auditor General of Canada <http://www.oag-bvg.gc.ca/internet/docs/20041102ce.pdf> (accessed January 16, 2009).

81 *A New Review Mechanism for the RCMP's National Security Activities*, p. 127.

review of national security responsibilities, with a focus on the propriety of such activities, including their legality, fairness and proportionality.

There is an equal need for oversight of the efficacy of the government's many national security activities. Commissioner O'Connor described the differences between propriety-based review and efficacy-based oversight. Review is conducted after the fact and "…at arm's length from both the management of the organization being reviewed and from the government."[82] It evaluates an agency's conduct against standards like lawfulness and/or propriety. In contrast, "…oversight mechanisms are often directly involved in the decision making of the organization they oversee":

> Involvement can be through setting standards against which the organization's activities are evaluated, pre-approving operations, implementing and enforcing recommendations, and/or imposing discipline. The organization's activities are sometimes assessed while they are going on. In their pure forms, oversight mechanisms can be seen as direct links in the chain of command or accountability: they both review and are responsible for the activities of the overseen body.[83]

Efficacy-based oversight focuses on whether the agencies have the competence and capacity to do their jobs and on whether their activities are sufficiently coordinated to accomplish the ultimate job of preventing terrorism. Such oversight is of critical importance.[84]

The NSA would be best positioned to conduct efficacy-based oversight. The NSA would have, under the new structure, access to all the information that is required to judge efficacy. Moreover, the NSA will have access to the Prime Minister, who might require improvements in the efficacy of the national security system. The deliberations of the NSA would be subject to the new national security privilege discussed above. Although the secrecy protected by such a privilege might limit the transparency that may be required for propriety-based review, secrecy will often be required in efficacy-based oversight.

The ability of the NSA to oversee the effectiveness of national security activities should not displace the responsibilities of ministers to ensure the efficient operation of the individual agencies and departments. The NSA should not hesitate to bring problems to the attention of the appropriate deputy minister or agency head for remedial action. However, the NSA should not be expected to supervise the details of the remedial action.

---

82 *A New Review Mechanism for the RCMP's National Security Activities*, pp. 456-457.

83 *A New Review Mechanism for the RCMP's National Security Activities*, p. 457.

84 Commissioner O'Connor did not dispute the importance of efficacy-based oversight, but believed that it was not within his mandate to make recommendations about reviewing the RCMP's national security activities.

2.3.3.8 Staffing the National Security Advisor's Office

The NSA should have a background in intelligence and a good understanding of the federal government and how law enforcement works. The NSA must also appreciate that there is no preferred response to terrorist threats, that each threat must be assessed individually and that the response must be tailored accordingly. The best individual from within or outside of government should be sought. An individual with these attributes will command the respect of the national security community and be able, as a result, to exercise the functions of the position independently and effectively.

The NSA should be appointed by the Prime Minister, preferably for a fixed term. A fixed term is useful to avoid the NSA becoming beholden to various interests. As well, a fixed term is necessary to avoid "burn out," as this will be one of the most demanding positions in government.

The NSA would receive information and advice from CSIS and from other agencies about threats to national security and would be responsible for determining how the government should respond. To do this, the NSA would need a modest full-time staff to assist in processing the advice provided by CSIS and in evaluating the merits of any proposed response.

The goal is to avoid a bureaucracy that duplicates that of other agencies. The purpose is to develop analysts who can support the NSA in serving the public interest – that is, serving without being blinkered by the vested interests of a particular agency.

The NSA will need a modest number of staff members who can advise about the efficacy of a specific government response to a threat. The NSA staff will also assist in preparing briefings for the Prime Minister. It will be for the NSA to determine the precise staffing requirements.

The NSA will need support in assessing the usefulness of passing the information to law enforcement agencies. The NSA should have secondees from the RCMP on staff.

The PCO structure supporting the NSA should be flexible enough to allow for hiring from the academic and private sectors and from abroad, as needed, and with appropriate security vetting. The NSA will also need adequate legal expertise, especially to address disputes that may arise in the relationship between intelligence and evidence. To this end, personnel from the office of the proposed Director of Terrorism Prosecutions should, if needed, be seconded to the staff of the NSA.[85]

---

85 See the discussion in Chapter III on the proposed Director of Terrorism Prosecutions.

2.3.3.9 Limits on the Role of the National Security Advisor: No Direct Budgetary or Personnel Control and Limited Operational Involvement

Hoffman's proposals that a national security coordinator have direct budgetary control over intelligence agencies and be able to hire and fire across the intelligence community[86] are not appropriate in the Canadian system, given that the NSA reports directly to the Prime Minister. In the Canadian tradition of parliamentary governance, an NSA with direct access to the Prime Minister would not necessarily require formal budgetary powers or personnel powers to exercise considerable authority. Although she advocated that budgeting decisions remain at the ministerial level, Bloodworth noted that the NSA could influence budgeting and high-level personnel decisions by way of access to the Prime Minister.

There may be merit in Rudner's proposal that the NSA have access to discretionary funds that could be allocated to agencies on a strategic basis.[87] The NSA would act as a transfer agency and the agency receiving the funds would remain accountable through ordinary channels about how it spent the funds.

The proposed NSA should not be involved in the day-to-day operations of the police, prosecuting and intelligence agencies. The NSA may, however, need to become involved in specific cases if they raise issues of policy, coordination, the resolution of disputes between the agencies or the need to intervene as part of effective oversight.

2.3.3.10 International Best Practices on Central Coordination of National Security Activities

The enhanced role for the NSA contemplated above is consistent with evolving international best practices.

In the United Kingdom, intelligence coordination is led by the Prime Minister's Security Adviser and Head of Intelligence, Security and Resilience, in the Cabinet Office. He chairs the Joint Intelligence Committee (JIC), the central agency of the government responsible for security and intelligence. The JIC has an analytical capacity and a coordinating role. The JIC does not override the decisions of the Director of the British Security Service (MI5), but has great influence.[88]

As in Canada, the central machinery is supported by the civil service in the form of an Intelligence and Security Secretariat, which is designed "…to ensure that the Prime Minister and other senior Ministers are well served on cross-Government

---

86 Testimony of Bruce Hoffman, vol. 94, December 12, 2007, pp. 12544-12545.

87 Rudner Paper on Building Counter-Terrorism Capacity, pp. 138-139.

88 Testimony of Martin Rudner, vol. 92, December 10, 2007, pp. 12256-12257. See also *National Intelligence Machinery*, pp. 20-27, online: Cabinet Office (United Kingdom) <http://www.cabinetoffice.gov.uk/media/136045/national_intelligence_booklet.pdf> (accessed July 28, 2009).

intelligence policy and security issues."[89] As in Canada, these forms of cross-governmental central coordination mirror similar intelligence coordination at lower levels. In Canada, this integration occurs through the Integrated Threat Assessment Centre and, in Britain, it occurs through the Joint Terrorism Analysis Centre. Although both bodies are located in intelligence agencies, both also involve the police.

In December 2008, after conducting a review of its national security activities, Australia appointed an NSA within the Prime Minister's Department with responsibilities for coordination matters. These included the training of executives in a whole-of-government approach and a more coordinated budgeting process to establish priorities across portfolios. The Australian NSA will also be responsible for an evaluation mechanism that will "…consider performance against whole-of-government outcomes in light of the priorities set out in the National Security Statement."[90] Australia's new NSA will also participate in a committee of secretaries or deputy ministers and will chair a national security intelligence coordination committee.[91] The Australian developments are notable because of their focus on the relationship between evidence and intelligence and the need for continuity of legal advice to both police forces and security intelligence agencies at all stages of terrorism investigations and prosecutions. The Australian developments are also notable for the role that an NSA located in the Prime Minister's Office can play in coordinating and evaluating national security activities from a whole-of-government perspective, and in view of the government's strategic priorities.

In the United States, the 9/11 Commission recommended greater integration of counterterrorism activities across the foreign/domestic divide as well as greater information sharing. Some of that Commission's proposals for more central oversight of intelligence by a Director of National Intelligence (DNI) were implemented in the *Intelligence Reform and Terrorism Prevention Act* of 2004.

It is clear that democracies are seeking to improve central coordination of national security activities. To achieve this, they are drawn to the idea of having a person at the centre with the authority to ensure coordination and resolve disputes among agencies, to establish and monitor the implementation of strategic security priorities, and to assess the efficacy of increasingly complex multi-agency national security systems.

2.3.3.11 Summary of the National Security Advisor's Enhanced Role

As former RCMP Commissioner Giuliano Zaccardelli testified, there is a need for someone with the necessary credibility and stature and who is not beholden to

89 "Directorate of Security and Intelligence," online: Cabinet Office (United Kingdom) <http://www.cabinetoffice.gov.uk/secretariats/intelligence_and_security.aspx> (accessed July 28, 2009).

90 Hon. Kevin Rudd, "The First National Security Statement to the Australian Parliament" (December 4, 2008), online: The Australian <http://www.theaustralian.news.com.au/files/security.pdf> (accessed July 31, 2009) [Rudd National Security Statement to Australian Parliament].

91 Rudd National Security Statement to Australian Parliament.

vested interests to bring the heads of sometimes warring agencies together and "…make them work for the good of Canada."[92] An NSA with an enhanced role could perform that function and bring the public interest to bear on thorny issues concerning: 1) strategic national security policies and priorities, 2) coordination of national security activities, 3) dispute resolution between agencies with national security responsibilities and 4) oversight of the effectiveness of the government's national security activities.

Recommendation 1:

The role of the National Security Advisor in the Privy Council Office should be enhanced. The National Security Advisor's new responsibilities should be as follows:

- to participate in setting strategic national security policies and priorities;
- to supervise and, where necessary, to coordinate national security activities, including all aspects of the distribution of intelligence to the RCMP and to other government agencies;
- to provide regular briefings to the Prime Minister and, as required, to other ministers;
- to resolve, with finality, disputes among the agencies responsible for national security;
- to provide oversight of the effectiveness of national security activities; and
- to carry out the government's national security policy in the public interest.

In carrying our these new duties, the National Security Advisor should be assisted by a Deputy and by a staff of secondees from agencies which have national security responsibilities, such as CSIS, the RCMP, the CBSA, and DFAIT. The National Security Advisor should continue to support relevant Cabinet committees and serve as Deputy Minister for the CSE, but these duties could, if necessary, be delegated to the Deputy National Security Advisor or to another official within the office of the NSA.

Measures to enhance the role of the NSA should not be delayed until the enactment of legislation on a new national security privilege.

---

92 Testimony of Giuliano Zaccardelli, vol. 86, November 30, 2007, pp. 11077-11081.

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

CHAPTER III: COORDINATING TERRORISM PROSECUTIONS

3.0 Introduction

Unlike most criminal investigations, terrorism investigations involve the use of secret intelligence from domestic and foreign sources. The decision to commence a terrorism prosecution arising from such investigations must be sensitive to the need to protect secret intelligence. Terrorism prosecutions also present formidable coordination issues because they can involve multiple police forces and multiple prosecuting agencies. Because of these coordination issues and the national and international implications of terrorism prosecutions, locating and centralizing them at the federal level is desirable.

The Attorney General of Canada plays an important role under section 38 of the *Canada Evidence Act*[1] by seeking to prevent disclosure of sensitive information to protect national security, national defence or international relations. These powers are not available to provincial Attorneys General or to the new federal Director of Public Prosecutions. As a result, any terrorism prosecution that raises the issue of disclosing secret intelligence will involve the Attorney General of Canada as a key participant.

Either a provincial Attorney General or the Attorney General of Canada must consent to the commencement of a terrorism prosecution – another distinction from many other criminal prosecutions.[2] This qualifies the traditional doctrine of police independence, which generally gives individual police officers the discretion to commence a prosecution by laying charges. This limitation on police independence stems from the danger that a terrorism prosecution could result in the disclosure of secret intelligence and could also disrupt ongoing security intelligence investigations.

Prosecutorial discretion is also affected by the unique characteristics of terrorism prosecutions. Although prosecutors must independently exercise their discretion with respect to the laying and continuation of charges, they may also require information from others in government to help inform their

---

1 R.S.C. 1985, c. C-5.
2 *Criminal Code*, R.S.C. 1985, c. C-46, s. 83.24 [*Criminal Code*].

exercise of discretion. It would be permissible for a minister or for the National Security Advisor (NSA), with the enhanced powers recommended for the NSA in this volume, to provide prosecutors with information about how a particular terrorism prosecution may affect the operations of a foreign or domestic security intelligence agency.

Terrorism prosecutions differ from other prosecutions because of the Attorney General of Canada's ability to take over prosecutions commenced by a provincial Attorney General.[3] This extraordinary federal power is related to the national significance of terrorism prosecutions and concerns about the possible disclosure of sensitive intelligence that Canada has produced or that it has received from its allies. In addition, terrorism prosecutions of the magnitude of the Air India trial would strain the resources of many provinces. For this reason, the federal government was heavily involved in the Air India trial through cost-sharing arrangements with British Columbia.

The Attorney General of Canada's critical role in terrorism prosecutions raises the question of whether he or she should be made responsible for all such prosecutions. A centralized approach of this nature would ensure a more coordinated and integrated handling of terrorism prosecutions. This would to some extent mirror the coordination role proposed for the NSA in Chapter II.

3.1 Limits on Police Discretion in Terrorism Investigations and Prosecutions

It can be argued that officials such as the NSA should not be involved in discussions of individual prosecutions, since this creates a risk of interference with police independence. However, such arguments often fail to take into account the parameters of police independence in the context of terrorism offences.

Police independence from government is an important principle. In the *Campbell* case, the Supreme Court of Canada recognized that "…[a] police officer investigating a crime is not acting as a government functionary or as an agent of anybody. He or she occupies a public office initially defined by the common law and subsequently set out in various statutes."[4] The Court stressed that it was dealing with an RCMP officer "…in the course of a criminal investigation, and in that regard the police are independent of the control of the executive government." This principle "…underpins the rule of law."[5] The Court added that, "…[w]hile for certain purposes the Commissioner of the RCMP reports to the Solicitor General, the Commissioner is not to be considered a servant or agent of the government while engaged in a criminal investigation. The Commissioner

---

3 *Security Offences Act*, R.S.C. 1985, c. S-7, s. 4 (ability of the Attorney General of Canada to prosecute offences that also constitute threats to the security of Canada); *Criminal Code*, s. 83.25(1) (ability of the Attorney General of Canada to prosecute terrorism offences).

4 *R. v. Campbell*, [1999] 1 S.C.R. 565 at para. 27.

5 [1999] 1 S.C.R. 565 at para. 29.

is not subject to political direction. Like every other police officer similarly engaged, he is answerable to the law and, no doubt, to his conscience."[6]
Justice Hughes, in his interim report on the 1997 APEC demonstrations in Vancouver, commented:

> In my view, there are compelling public policy reasons not to extend the concept of police independence beyond that set out in *Campbell*. The issue is one of balance. It is clearly unacceptable for the federal government to have the authority to direct the RCMP's law enforcement activities, telling it who to investigate, arrest and prosecute, whether for partisan or other purposes. At the same time, it is equally unacceptable for the RCMP to be completely independent and unaccountable, to become a law unto themselves.[7]

Commissioner O'Connor recognized the danger of government direction of police investigations:

> If the Government could order the police to investigate, or not to investigate, particular individuals, Canada would move towards becoming a police state in which the Government could use the police to hurt its enemies and protect its friends, rather than a free and democratic society that respects the rule of law.[8]

This understanding of police independence is consistent with that articulated in 1981 by the McDonald Commission, which stressed that ministers have no right to direct the RCMP in its use of powers of investigation, arrest and prosecution.[9] However, Commissioner O'Connor noted that police independence cannot be absolute. Otherwise, it "…would run the risk of creating another type of police state, one in which the police would not be answerable to anyone."[10]

---

6 [1999] 1 S.C.R. 565 at para. 33.

7 Commission for Public Complaints Against the RCMP, RCMP Act-Part VII Subsection 45.45(14), Commission Interim Report Following a Public Hearing Into the Complaints regarding the events that took place in connection with demonstrations during the Asia Pacific Economic Cooperation Conference in Vancouver, BC in November 1997 at the UBC Campus and at the UBC and Richmond detachments of the RCMP (Ottawa: RCMP Public Complaints Commission, 2001), pp. 83-84.

8 Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (Ottawa: Public Works and Government Services Canada, 2006), p. 458 [*A New Review Mechanism for the RCMP's National Security Activities*].

9 Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Freedom and Security under the Law*, Second Report - vol. 2 (Ottawa: Supply and Services Canada, 1981), p. 1013 [*Freedom and Security under the Law]*.

10 *A New Review Mechanism for the RCMP's National Security Activities*, p. 460.

The principle of police independence has been qualified in the national security context:

> ….the RCMP and other police forces must have the Attorney General's consent before laying charges for a terrorism offence under the *Criminal Code* or the *Security of Information Act*, and before using the extraordinary police powers of investigative hearings or preventative arrests related to terrorism investigations. As this approval requirement relates directly to individual criminal investigations, it can be seen as a restraint on the doctrine of police independence.[11]

Although statutory provisions authorizing preventive arrests and investigative hearings have now been repealed, the requirement that the Attorney General of Canada or a provincial Attorney General consent to the laying of charges for a terrorism offence remains under section 83.24 of the *Criminal Code*.[12]

What is the rationale for limiting the independence of police officers to lay charges in terrorism cases? One is that the requirement for the Attorney General's prior consent will help to ensure that serious terrorism charges are laid only in appropriate cases. Certain other *Criminal Code* offences similarly require the consent of the Attorney General before charges are laid.[13] Another rationale, unique to the national security context, is that requiring the Attorney General's consent can assist in managing the relationship between intelligence and evidence. Normally, a police officer has full discretion to lay charges, which could subsequently be stayed by the Attorney General or his or her authorized delegate. The public act of laying charges in the national security context could, however, compromise the secrecy of ongoing intelligence investigations.

The requirement for the Attorney General to consent to the laying of charges gives the Attorney General the chance to prevent the laying of charges if, in his or her view, the public interest lies in continuing an intelligence investigation or in protecting intelligence, including the identities of providers of intelligence, such as human sources, from the risk of being disclosed in a terrorism prosecution. The ability of the Attorney General to prevent the laying of charges on such a basis also contemplates that the Attorney General will have access to relevant information about intelligence investigations and about the risks that could flow from the disclosure of intelligence.

The O'Connor Commission noted how, within the RCMP, the increased central oversight of national security investigations placed appropriate limits on individual police officers.

---

11 *A New Review Mechanism for the RCMP's National Security Activities*, p. 460.

12 R.S.C. 1985, c. C-46. The consent of the Attorney General of Canada must be obtained to lay charges under the Security of Information Act: R.S.C. 1985, c. O-5, s. 24.

13 See, for example, ss. 318(3) and 319(6).

Central oversight within the RCMP does not raise the same constitutional concerns about limiting police discretion. It reflects the fact that national security policing may have broader implications than other forms of policing. Unlike other criminal investigations, national security investigations could affect security intelligence agencies and even Canada's relations with other countries. There are good reasons why individual police officers should not have the ability unilaterally to commence a complex terrorism prosecution that could have an impact on agencies both inside and outside Canada.

The mere fact that the additional powers proposed by the Commission for the NSA would enable it to compel CSIS to provide intelligence information to the RCMP would not compromise police independence. The expanded role of the NSA would not involve directing the police about the conduct of their terrorism investigations or about possible charges. It would simply permit the NSA to require that information be given to the RCMP, where appropriate. The police would remain free to do what they wished with information provided by the NSA.

Other authorities on police-government relations have recognized that the responsible minister can interact with the police without undermining police independence. For example, Commissioner O'Connor noted that, "… [w]hile direction of operational matters is more controversial, I agree with the McDonald Commission that, if it raises an important question of public policy…. [the Minister] may give guidance to the [RCMP] Commissioner and express to the Commissioner the government's view of the matter."[14] The McDonald Commission, in turn, drew a distinction between the impropriety of the responsible minister directing the RCMP about law enforcement powers of investigation, arrest and prosecution, and the legitimate ability of the minister to be "…informed of any operational matter, even one involving an individual case, if it raises an important question of public policy. In such cases, he may give guidance to the [RCMP] Commissioner and express to the Commissioner the government's view of the matter, but he should have no power to give *direction* to the Commissioner."[15]

The NSA should have the same powers as the responsible minister when it comes to informing the RCMP about policy matters that may arise in particular investigations. Indeed, the enhanced powers of the NSA proposed in this volume would allow the NSA to inform the RCMP about policy matters from the unique perspective of the NSA, situated at the centre of government.

Concerns about the NSA interfering with police independence are also lessened because the police do not have their traditional powers to lay charges when terrorism offences under the *Criminal Code* are involved. As discussed earlier, the police require the consent of an Attorney General to lay a terrorism charge.[16]

---

14 *A New Review Mechanism for the RCMP's National Security Activities*, p. 463.
15 Freedom and Security under the Law, Second Report - vol. 2, p. 1013.
16 *Criminal Code*, s. 83.24.

Thus, the ultimate act of independence of the police, the ability of an individual police officer to lay charges, has already been reduced.

A second problem addressed by the principle of police independence is the risk of political interference through the placement of limitations on investigations and on decisions to lay charges to protect friends of the government. Such interference would undermine the rule of law, which requires that the law apply to all individuals. This dimension of police independence, however, can create some difficulties in national security matters because the NSA and others in government may have intelligence, including intelligence obtained from other governments, that may be relevant to an ongoing police investigation, but that cannot be disclosed to the police because of the risk that it will have to be made public.

The NSA could help to resolve disputes that may arise between CSIS and the RCMP about terrorism investigations. It may even be appropriate for the NSA to communicate to all relevant parties, including the RCMP, the Government's views about the merits of a prosecution instead of a measure that maintains the secrecy of intelligence and ongoing investigations.

The idea that the police should be informed about the Government's views on a criminal matter is not without critics. Ontario's Ipperwash Inquiry recommended that the responsible minister should "…not have the authority to offer 'guidance' as opposed to 'direction.'"[17] The reforms proposed by this Commission do not contemplate the NSA providing "guidance" or "direction" to the police, but merely information.

Preventing the government from making its views known to the police in national security cases would be unworkable. Police actions in the national security field can have unanticipated effects on Canada's relations with other states, on national defence and on multilateral security intelligence investigations. Police actions may also affect the information that must be disclosed in subsequent prosecutions and the actions that the Attorney General of Canada may have to take under section 38 of the *Canada Evidence Act* to protect information from disclosure. The need to take these issues into account suggests that police and prosecutors require relevant information from the Government of Canada.

3.2 The Role of Prosecutorial Discretion in Terrorism Cases

Managing the difficult relationship between intelligence and evidence is not only made more complicated by concerns about police discretion and independence, but also by concerns about the independence of the Attorney General and prosecutors. It is a constitutional principle that the Attorney General is independent from the Cabinet in which he or she sits when exercising prosecutorial discretion about bringing or continuing a prosecution. The

17 *Report of the Ipperwash Inquiry*, vol. 2 - Policy Analysis (Toronto: Ministry of the Attorney General, 2007), p. 358.

Supreme Court of Canada explained that "…[t]he gravity of the power to bring, manage and terminate prosecutions which lies at the heart of the Attorney General's role has given rise to an expectation that he or she will be in this respect fully independent from the political pressures of the government."[18]

However, independence has never meant that the Attorney General cannot receive relevant information from the Prime Minister and other Cabinet colleagues. Lord Shawcross, in a famous statement concerning the proper approach to the Attorney General's independence, drew an important distinction between the Attorney General's practical and proper need to seek information from Cabinet colleagues that may be relevant to exercising prosecutorial discretion, and the impropriety of taking instructions about the exercise of prosecutorial discretion.[19]

The ability of the Attorney General to engage in consultations with others, and to obtain relevant information from them, is of particular importance in the national security field where a terrorism prosecution may implicate intelligence and foreign policy considerations well beyond the Attorney General's traditional area of expertise. To paraphrase from the more colourful parts of the famous statement by Lord Shawcross, the Attorney General would "in some cases be a fool" if he or she did not to consult with Cabinet colleagues who have important information that will be relevant to the discharge of prosecutorial duties in national security matters.[20] Indeed, in exceptional cases, the Attorney General might need to receive information about the fate of hostages or about vital

---

18 *Krieger v. Law Society of Alberta*, 2002 SCC 65, [2002] 3 S.C.R. 372 at para. 29.

19 "The true doctrine," according to Lord Shawcross, "is that it is the duty of the Attorney General, in deciding whether or not to authorize the prosecution, to acquaint himself with all the relevant facts, including, for instance, the effect which the prosecution, successful or unsuccessful as the case may be, would have upon public morale and order, and with any other consideration affecting public policy. In order so to inform himself, he may, although I do not think he is obliged to, consult with any of his colleagues in government, and indeed, as Lord Simon once said, he would in some cases be a fool if he did not. On the other hand, the assistance of his colleagues is confined to informing him of particular considerations which might affect his own decision, and does not consist, and must not consist, in telling him what that decision ought to be": John Ll. J. Edwards, *The Attorney General, Politics and the Public Interest* (London: Sweet & Maxwell, 1984), pp. 318-319 [Edwards, *The Attorney General, Politics and the Public Interest*]. A Canadian Attorney General, Ron Basford, adopted this pronouncement in the context of explaining a decision whether to consent to a prosecution under the *Official Secrets Act* when he stated: "In arriving at a decision on such a sensitive issue as this, the Attorney General is entitled to seek information and advice from others but in no way is he directed by his colleagues in the government or by Parliament itself.": Edwards, *The Attorney General, Politics and the Public Interest*, pp. 359-360.

20 Edwards, *The Attorney General, Politics and the Public Interest*, p. 319. Although he admits that the line between receiving factual information and opinions from other ministers about what action should be taken is difficult "…to sustain with the required degree of certainty that gives the appearance of stating a fundamental principle,," Edwards interprets Lord Shawcross' famous statements as making "constitutionally improper" "…the expression by the Prime Minister, another minister or the government of their individual or collective view on the question whether or not the Attorney General should prosecute.": Edwards, *The Attorney General, Politics and the Public Interest*, pp. 323-324.

information-sharing arrangements with foreign countries in order to be fully informed in exercising prosecutorial discretion.[21]

In most cases, the role of the NSA would be to inform the Attorney General of Canada or the relevant provincial Attorney General of the unforeseen consequences of proceeding with a terrorism prosecution. Information from the NSA might be equally important where a provincial Attorney General is considering whether to consent to a terrorism offence prosecution.

The exclusive authority of the Attorney General of Canada to seek non-disclosure orders and issue non-disclosure certificates under section 38 of the *Canada Evidence Act* as well as the national implications of terrorism prosecutions justify early federal involvement in terrorism prosecutions. It makes little sense for a provincial Attorney General to consent to a terrorism prosecution without knowing the position the Attorney General of Canada will take on section 38 national security confidentiality matters – matters which can have a critically important impact on a prosecution. In addition, the Attorney General of Canada can invoke powers under section 2 of the *Security Offences Act*[22] to assume control of terrorism prosecutions. This includes the power to stop such prosecutions. The ultimate decision and accountability for the laying of terrorism charges and terrorism prosecutions, however, depends on the independent judgment of the relevant provincial Attorney General or the Attorney General of Canada. Still, the Attorney General will often require information and even guidance from the Government of Canada.

Recommendation 2:

The role of the National Security Advisor should be exercised in a manner that is sensitive to the principles of police and prosecutorial independence and discretion, while recognizing the limits of these principles in the prosecution of terrorism offences. The principle of police independence should continue to be qualified by the requirement that an Attorney General consent to the laying of charges for a terrorism offence.

The Attorney General of Canada should continue to be able to receive relevant information from Cabinet colleagues, including the Prime Minister and the National Security Advisor, about the possible national security and foreign policy implications of the exercise of prosecutorial discretion.

---

21 Edwards describes as "clearly defensible" an instance in which the Attorney General in England met with the Lord Chancellor, the Prime Minister and other ministers in forming an opinion as to how charging and bringing to trial a hijacker would affect the lives of hostages: Edwards, *The Attorney General, Politics and the Public Interest*, pp. 324-325. This passage was quoted with approval in a recent case affirming the lawfulness of a decision not to prosecute bribery charges, in part because of information that a prosecution would lead to less information sharing by the government of Saudi Arabia and would put British lives at risk. *R (on the application of Corner House Research and Others) v. Director of the Serious Fraud Office*, [2008] UKHL 60 at para. 39.

22 R.S.C. 1985, c. S-7.

3.3 The Role of the Federal Director of Public Prosecutions in Terrorism Prosecutions

In 2006, Parliament enacted the *Director of Public Prosecutions Act* as part of the *Federal Accountability Act*.[23] The *Director of Public Prosecutions Act* provides for the appointment of a Director of Public Prosecutions (DPP) by the Attorney General of Canada.[24] The DPP holds office for seven years and can be dismissed with cause through a resolution of the House of Commons.[25]

The DPP is an entity separate from the Attorney General of Canada and is empowered to initiate and conduct prosecutions on behalf of the Attorney General. The Attorney General may issue directives in writing to the DPP under section 10 of the Act. Sections 13 and 14 contemplate that the DPP will inform the Attorney General of any prosecution that "…raises important issues of general interest" and that the Attorney General may make a separate intervention in such proceedings. In addition, the Attorney General of Canada has the authority, under section 15 of the Act, to assume conduct of a prosecution, but only after consulting the DPP and issuing a "...notice of intent to assume conduct of the prosecution" and publishing the notice in the *Canada Gazette*.

Whatever the merits of the *Director of Public Prosecutions Act* for other criminal prosecutions, it causes considerable coordination problems for terrorism prosecutions.

Terrorism prosecutions are more complex than other criminal prosecutions – in no small part because of the critical role of section 38 of the *Canada Evidence Act*. Under section 38, the Attorney General of Canada has exclusive jurisdiction to make decisions about the disclosure of information that, if disclosed, could cause harm to national security, national defence or international relations. Managing the relationship between intelligence and evidence is difficult enough without in addition dividing the prosecution process into two parts by having the DPP conduct the prosecution and the Attorney General of Canada make decisions under section 38. Like the process in which the Federal Court decides non-disclosure issues under section 38 and the criminal trial court decides whether a remedy is necessary to respond to non-disclosure, a prosecution process divided into two parts causes needless complexity in terrorism prosecutions. It makes it unclear who is in charge and it diffuses responsibility.

In particular, the division of prosecutorial responsibilities raises concerns that the Attorney General of Canada may seek a non-disclosure order under section 38 without sufficiently understanding the possible effect of the order on the viability of a prosecution. After all, the trial judge has an obligation to provide remedies in response to any non-disclosure order, possibly including a stay of

---

23 S.C. 2006, c. 9, s. 121.
24 *Director of Public Prosecutions Act*, S.C. 2006, c. 9, s. 121, s. 4 [Director of Public Prosecutions Act].
25 *Director of Public Prosecutions Act*, s. 5(1).

proceedings, to protect the accused's right to a fair trial.[26] This division in turn causes problems for prosecutors. As the narrative contained in this report about the Reyat prosecution reveals, a provincial prosecutor, James Jardine, had difficulty anticipating the position that CSIS and the Attorney General of Canada would take about disclosing CSIS intelligence, even though this disclosure issue could be critical to the viability of the prosecution.

The typical justification for dividing functions is that it creates a form of checks and balances. However, the case for such checks and balances is unclear in the context of terrorism prosecutions. It cannot be argued that the Director of Public Prosecutions will be more attentive than the Attorney General of Canada to disclosure obligations; the Attorney General has a long-established role to ensure that justice is done.[27] It is important that the prosecutor who commences a terrorism prosecution be fully informed from the start about the disclosure implications of the prosecution. It should not be appropriate for a prosecutor to dismiss the issue of protecting secrets by arguing that protection is someone else's job. The idea that a particular issue was "someone else's job," unfortunately, ran through most of the Air India investigations and prosecutions.

While there may be other options, the preference of the Commission is to give the Attorney General of Canada the power to conduct terrorism prosecutions, in addition to exercising current powers under section 38 relating to the disclosure of intelligence. The most practical and efficient response would be for the Attorney General of Canada to publish a directive, setting out a new policy that the Attorney General, not the DPP, would conduct all future terrorism prosecutions. This could be done immediately without amending either the *Director of Public Prosecutions Act* or the *Department of Justice Act*,[28] although it may be desirable to amend those acts eventually to reflect this new arrangement.

Parliament's decision to give the Attorney General of Canada unique powers and responsibilities under section 38 should be respected. The Attorney General of Canada is in the best position to balance the competing demands for disclosure and secrecy.

3.3.1 The Need for a Specialized Director of Terrorism Prosecutions

There is a need for expertise in terrorism prosecutions. Terrorism prosecutions can involve multiple complex charges under the *Anti-terrorism Act*,[29] as well as complex issues under section 38 of the *Canada Evidence Act* about the appropriate balance between secrecy and disclosure. The 2007-08 Annual Report of the Public Prosecution Service of Canada indicates that only three per cent of in-house counsel time within the Service was devoted to terrorism

---

26 *Canada Evidence Act*, R.S.C. 1985, c. C-5, s. 38.14.

27 See *R. v. Stinchcombe*, [1991] 3 S.C.R. 326 at 333, referring to the statement of Rand J. in *Boucher v. The Queen*, [1955] S.C.R. 16 at 23-24.

28 R.S.C. 1985, c. J-2.

29 S.C. 2001, c. 41.

prosecutions.[30] It would be advisable to establish a position of Director of Terrorism Prosecutions, serving under the Attorney General of Canada, to create a pool of experienced counsel for terrorism prosecutions. This small team of counsel could also provide legal advice about the conduct of national security confidentiality proceedings under section 38 and give legal advice to agencies that collect intelligence and evidence in terrorism investigations.

The Attorney General of Canada should be able to communicate with the office of the Director of Terrorism Prosecutions without the need for public directives like those contemplated under the *Director of Public Prosecutions Act*. Directives are not advisable in terrorism prosecutions where issues, such as the decision about whether to prosecute or the choice of charge, may depend on the ability to protect intelligence from disclosure. Full, frank and confidential discussions are needed about the appropriate balance between secrecy and disclosure in terrorism cases.

The office of the Director of Terrorism Prosecutions should not be a large bureaucracy. The Director would be appointed by the Attorney General of Canada and, when appropriate, would work closely with the Attorney General and with the Deputy Attorney General. The Director of Terrorism Prosecutions should serve at the pleasure of the Attorney General of Canada. The office of the Director of Terrorism Prosecutions should, where appropriate, be able to draw on expertise from the provinces and the private sector, as well as from the Public Prosecution Service of Canada.

The lawyers in the office of the Director of Terrorism Prosecutions could provide advice both to CSIS and to the RCMP about terrorism investigations and they would conduct all aspects of terrorism prosecutions, including handling matters under section 38 of the *Canada Evidence Act*.

The Director of Terrorism Prosecutions would also meet with provincial Attorneys General to coordinate prosecutorial actions in terrorism matters. There is a danger that this coordination might not be given priority if terrorism prosecutions continue to be conducted by the Public Prosecution Service of Canada, where they would involve only a very small fraction of overall prosecutorial time. The placement of the Director of Terrorism Prosecutions within the Attorney General of Canada's department should also facilitate the necessary political cooperation and negotiations with the provinces about the division of responsibilities, cost-sharing and related matters.

The Director of Terrorism Prosecutions could assume responsibility for federal involvement in terrorism prosecutions, supplying related legal advice to Integrated National Security Enforcement Teams (INSETs) and legal advice about the counterterrorism work of the RCMP and CSIS. At present, the RCMP and CSIS

---

30 Public Prosecution Service of Canada, Public Prosecution Service of Canada Annual Report 2007-2008, p. 8, online: Public Prosecution Service of Canada <http://www.ppsc-sppc.gc.ca/eng/pub/ar08-ra08/ar08-ra08.pdf> (accessed July 28, 2009).

receive inadequate legal advice on such matters from "in-house" counsel because of the limited number of lawyers dedicated to these issues. A lack of continuity and consistency in legal advice has contributed to misunderstandings about complex disclosure obligations, which in turn has hindered the relationship between the RCMP and CSIS.[31] There is a need for continuity of legal advice in terrorism investigations, from the initial collection of intelligence and evidence through to the completion of prosecutions. The agencies involved should have a single source of reliable legal advice.

The Director of Terrorism Prosecutions could provide legal advice from investigation to prosecution to ensure that the perspectives of CSIS and others about disclosure are fully understood by those involved. The overarching role of the Director would preclude the danger that lawyers representing CSIS and those representing the RCMP might simply pursue their client agency's interests about secrecy or disclosure, regardless of the broader public interest. The Director would seek to understand both CSIS and RCMP perspectives on disclosure, but would make a decision in the public interest.

The Director of Terrorism Prosecutions would also, of necessity, be involved in the pre-charge screening of terrorism cases because of the requirement that the Attorney General consent to prosecutions of terrorism offences. There may be concerns about prosecutorial involvement at both the investigative and charging stages. However, terrorism prosecutions can raise issues of such legal complexity that there is a need for continuity of expert legal advice from investigation through to prosecution.

One limit should be placed on the Director of Terrorism Prosecution's ability to provide legal services in terrorism matters. As the narrative of this report notes, counsel representing the Government of Canada in civil litigation arising from the Air India bombing was present at several critical meetings concerning the Air India prosecution. Although there was evidence that civil litigation counsel was instructed to place the interests of the prosecution before those of the civil lawsuit, considerations of civil liability do not easily mix with the need to exercise prosecutorial discretion in the public interest. Hence, to avoid a conflict of interest, or the appearance of a conflict, the Director should preferably not represent the Government of Canada in a civil lawsuit.

The Director of Terrorism Prosecutions, like all representatives of the Attorney General of Canada, should exercise prosecutorial functions in an objective, independent and even-handed manner consistent with the traditions of the office of the Attorney General.[32]

Establishing dedicated expertise in terrorism prosecutions accords with best practices in other countries. For example, the British Crown Prosecution Service has a dedicated Counter Terrorism Division, centralized in London, to conduct

---

31 Security Intelligence Review Committee, *CSIS Cooperation with the RCMP - Part I* (SIRC Study 1998-04), October 16, 1998, p. 18 [SIRC Study 1998-04].

32 *R. v. Regan*, 2002 SCC 12, [2002] 1 S.C.R. 297.

terrorism prosecutions.[33] This Service handles both terrorism prosecutions and public interest immunity applications that attempt to shield intelligence from disclosure. In the United States, a National Security Division has been created in the Department of Justice to consolidate national security operations.[34] This Division assists intelligence agencies in many matters, including warrant applications, and helps during prosecutions with respect to the disclosure of intelligence. The Division also deals with international cooperation in terrorism prosecutions and with policy matters involving counterterrorism.

Recommendation 3:

Terrorism prosecutions at the federal level should be supervised and conducted by a Director of Terrorism Prosecutions appointed by the Attorney General of Canada.

Recommendation 4:

The office of the Director should be located within the department of the Attorney General of Canada and not within the Public Prosecution Service of Canada. The placement of the proposed Director of Terrorism Prosecutions in the Attorney General's department is necessary to ensure that terrorism prosecutions are conducted in an integrated manner, given the critical role of the Attorney General of Canada under the national security confidentiality provisions of section 38 of the *Canada Evidence Act*.

Recommendation 5:

The Director of Terrorism Prosecutions should also provide relevant legal advice to Integrated National Security Enforcement Teams and to the RCMP and CSIS with respect to their counterterrorism work to ensure continuity and consistency of legal advice and representation in terrorism investigations and prosecutions.

Recommendation 6:

The Director of Terrorism Prosecutions should preferably not provide legal representation to the Government of Canada in any civil litigation that might arise from an ongoing terrorism investigation or prosecution, in order to avoid any possible conflict of interest.

---

33 The Crown Prosecution Service (United Kingdom), "Prosecuting terrorists - Counter Terrorism Division," online: The Crown Prosecution Service (United Kingdom) <http://www.cps.gov.uk/your_cps/ctd.html> (accessed July 31, 2009).

34 United States Department of Justice, National Security Division, "Mission and Functions," online: United States Department of Justice <http://www.usdoj.gov/nsd/mission_functions.htm> (accessed July 28, 2009).

3.3.2 The Role of Provincial and Territorial Attorneys General in Terrorism Prosecutions

A logical solution to the difficulties of coordinating terrorism prosecutions would be to recommend that the Attorney General of Canada exercise his or her fiat under section 2 of the *Security Offences Act* to conduct all terrorism prosecutions on the basis that crimes of terrorism constitute threats to the security of Canada. This would keep the difficult coordination issues in the relationship between terrorism prosecutions and national security confidentiality proceedings under section 38 of the *Canada Evidence Act* within the federal government. It would also recognize that terrorism has the potential to affect the political, social and economic life of the entire nation.

However, Canada has never been a country governed solely by logic. The *Anti-terrorism Act* gave both federal and provincial Attorneys General the authority to prosecute terrorism offences. As the Air India prosecution revealed, there is considerable prosecutorial experience and talent at the provincial level. In addition, there has been cooperation between federal and provincial Attorneys General during a number of contemporary terrorism prosecutions. No evidence has been presented that the provincial role in terrorism prosecutions has presented a problem in any prosecution. For this reason, there is no justification at this time for ending the provincial role in terrorism prosecutions.

Still, evidence has been presented about the challenges, including costs, that a complex terrorism prosecution may present for many provinces. Many provinces might be willing to agree in advance to a significant, or even exclusive, federal role in terrorism prosecutions. No provincial Attorney General made submissions to the Commission about the provincial role in terrorism prosecutions. This absence of interest may suggest that most provinces would be prepared to cede their prosecutorial powers to a new federal Director of Terrorism Prosecutions. In any event, the Attorney General of Canada can exercise his or her fiat under section 2 of the *Security Offences Act* to pre-empt or to take over a provincial terrorism prosecution.

This Director of Terrorism Prosecutions should come to understandings with provincial Attorneys General about a coordinated approach to terrorism prosecutions, including possible advance agreements that the Attorney General of Canada will conduct terrorism prosecutions in a given province. There should also be advance discussions of other aspects of the federal role, including federal cost-sharing.

Recommendation 7:

A lead federal role in terrorism prosecutions should be maintained because of their national importance and the key role that the Attorney General of Canada will play in most terrorism prosecutions under section 38 of the *Canada Evidence Act*. The Attorney General of Canada should be prepared to exercise the right under the *Security Offences Act* to pre-empt or take over provincial

terrorism prosecutions if the difficulties of coordinating provincial and federal prosecutorial decision-making appear to be sufficiently great or if a federal prosecution is in the public interest.

3.3.3 The Need for Provincial Authorities to Notify Federal Authorities about Possible Terrorism Prosecutions

Provincial Attorneys General should notify the Director of Terrorism Prosecutions of any terrorism prosecution that they are considering. This is necessary to ensure advance notice to the Attorney General of Canada of any proceedings involving sensitive or potentially injurious information. In fact, section 38.02 of the *Canada Evidence Act* currently requires provincial Attorneys General to give notice of such proceedings to the Attorney General of Canada.

Notifying the Director of Terrorism Prosecutions in advance of any potential prosecution involving a terrorist group or a terrorist activity would also provide an opportunity for the Director to consider how the provincial prosecution accords with the overall strategy at the federal level about a particular threat to the security of Canada. The Director, in consultation with the NSA, would be able to advise whether a prosecution might be premature – for instance, if a provincial prosecution might disrupt an ongoing security intelligence investigation being conducted with foreign agencies.

The Director of Terrorism Prosecutions would also be in a good position to advise about the merits of prosecuting an offence under the terrorism provisions of the *Criminal Code*, or under other Code provisions not specifically related to terrorism. For example, a prosecution of a non-terrorist criminal offence might make it easier to protect sensitive intelligence from disclosure. The Director of Terrorist Prosecutions could also seek advice from the NSA about viable alternatives to prosecutions. As discussed in Chapter II, these alternatives could include immigration proceedings, the freezing or forfeiture of terrorist assets, the revocation of charitable status or simply the continued surveillance of a terrorist suspect to build a better case.

A requirement that the provinces consult with the federal authorities might have made a difference in the 1986 prosecution of Reyat and Parmar about the use of explosives in Duncan. This prosecution was commenced while the investigation of the Air India bombing was still at a preliminary stage. The failure to consult may have been the reason that no evidence was called against Parmar, the suspected ringleader of the bombing, and only a $2000 fine was levied against Reyat, who was subsequently convicted of manslaughter, first in relation to the Narita bombing and later in relation to the Flight 182 bombing. The Duncan Blast prosecution was, in the Commission's view, premature and not in the public interest.

Recommendation 8:

Provincial Attorneys General should notify the Attorney General of Canada through the proposed federal Director of Terrorism Prosecutions of any potential prosecution that may involve a terrorist group or a terrorist activity, whether or not the offence is prosecuted as a terrorism offence. The National Security Advisor should also be notified.

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

CHAPTER IV: THE COLLECTION AND RETENTION OF INTELLIGENCE: MODERNIZING THE *CSIS ACT*

4.0 Introduction

The RCMP had the responsibility to investigate and prevent terrorist acts, including conspiracies, counselling and attempts to commit murder, even before the *Anti-terrorism Act*[1] created new crimes relating to the financing and facilitation of terrorist activities and participation in terrorist groups.[2]

CSIS was created in 1984 with a mandate to provide the Government of Canada with advice about threats to the security of Canada, including the threat posed by terrorism. The creation of CSIS was also a response to revelations of wrongdoing by the RCMP Security Service and the consequent recommendations of the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (McDonald Commission). CSIS was designed to be a civilian security agency, without law enforcement powers, which would be subject to greater political direction and review and oversight than the police.[3] CSIS was authorized to collect information and intelligence about activities that might, on reasonable grounds, be suspected of constituting threats to the security of Canada, to the extent that it was strictly necessary, and to report to and advise the Government about such threats.[4] CSIS could also obtain judicial warrants to conduct searches and electronic surveillance when the Director of CSIS believed, on reasonable grounds, that a warrant was required to investigate a threat to the security of Canada.[5]

---

1 S.C. 2001, c. 41.

2 Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (Ottawa: Public Works and Government Services Canada, 2006), p. 313 [*Report of the Events Relating to Maher Arar: Analysis and Recommendations*].

3 Wesley Wark, "The Intelligence-Law Enforcement Nexus: A study of co-operation between the Canadian Security Intelligence Service and the Royal Canadian Mounted Police, 1984-2006, in the Context of the Air India terrorist attack" in Vol. 1 of Research Studies: Threat Assessment RCMP/CSIS Co-operation, pp. 150-151 [Wark Paper on Intelligence-Law Enforcement Nexus].

4 *CSIS Act*, R.S.C. 1985, c. C-23, s. 12 [*CSIS Act*].

5 *CSIS Act*, s. 21.

The *Security Offences Act*[6] was enacted in 1984 as companion legislation to the *CSIS Act*.[7] It recognized the continued role of law enforcement in national security matters. It gave the RCMP and the Attorney General of Canada the lead role in investigating and prosecuting crimes that also constituted threats to the security of Canada as defined in the *CSIS Act*. The *CSIS Act* contemplated that CSIS would share information with the police.[8] Together, the two acts recognized that CSIS would sometimes need to work with law enforcement agencies because CSIS did not have powers to arrest and detain people who might be about to commit, or who had committed, crimes.

The Attorney General of Canada submitted to this Commission that post-McDonald Commission reforms gave the RCMP and CSIS "…separate but complementary mandates concerning threats to national security."[9]

Although the *CSIS Act*, combined with the *Security Offences Act*, contemplated the interchange of information between CSIS and the RCMP about threats to the security of Canada that were also crimes, the *CSIS Act* was not formulated with the particular challenges of terrorism prosecutions in mind. The Cold War was still seen as the dominant threat to Canadian security.[10] The terrorist acts that did occur during that period – such as the bombing of Litton Systems by Direct Action and a series of attacks, including murders and hostage taking, directed against Turkish interests in Canada – did not have a major impact on Canadians or on policy-making.[11]

The *CSIS Act* was not substantively amended even after the events of 9/11. This raises the question of whether the Act, now a quarter century old, should be modernized. Does it need to reflect the new emphasis on terrorism, fundamental changes to Canada's laws and developments in *Charter* jurisprudence, as well as the enactment of new terrorist crimes? These are the dominant questions examined in this chapter.

4.1 No Absolute Secrecy and No Wall between Intelligence and Evidence

The *CSIS Act* never contemplated absolute secrecy or a wall protecting secret intelligence from being used as evidence by police and prosecutors. Section 19(2) provides that CSIS "may disclose information" to police officers or to federal or provincial Attorneys General for use in investigations or prosecutions. Section 18 contemplates that, while CSIS intelligence and the identity of CSIS

---

6 R.S.C. 1985, c. S-7.
7 R.S.C. 1985, c. C-23.
8 *CSIS Act*, s. 19.
9 Final Submissions of the Attorney General of Canada, Vol. I, February 29, 2008, para. 38 [Final Submissions of the Attorney General of Canada].
10 Peter M. Archambault, "Context Is Everything: The Air India Bombing, 9/11 and the Limits of Analogy" in Vol. 1 of Research Studies: Threat Assessment RCMP/CSIS Co-operation, p. 85.
11 David A. Charters, "The (Un)Peaceable Kingdom? Terrorism and Canada before 9/11 (October 2008) 9(4) *IRPP Policy Matters*.

confidential sources and covert agents should normally be kept secret, this information could be provided to others for various reasons, including for its use in criminal investigations and prosecutions. Such sharing of intelligence would then make CSIS information susceptible to public disclosure.

Unfortunately, the implications of these provisions providing for interchange between CSIS and the police were not adequately appreciated when they were enacted. For example, an influential 1983 report by a Special Senate Committee chaired by Senator Michael Pitfield stressed the differences between law enforcement and intelligence. It defined law enforcement as "essentially reactive," ignoring the proactive role of the police in preventing crime and investigating conspiracies and attempts:

> Law enforcement is essentially reactive. While there is an element of information-gathering and prevention in law enforcement, on the whole it takes place after the commission of a distinct criminal offence. The protection of security relies less on reaction to events; it seeks advance warning of security threats, and is not necessarily concerned with breaches of the law. Considerable publicity accompanies and is an essential part of the enforcement of the law. Security intelligence work requires secrecy. Law enforcement is 'result-oriented', emphasizing apprehension and adjudication, and the players in the system - police, prosecutors, defence counsel, and the judiciary - operate with a high degree of autonomy. Security intelligence is, in contrast, 'information-oriented'. Participants have a much less clearly defined role, and direction and control within a hierarchical structure are vital. Finally, law enforcement is a virtually 'closed' system with finite limits - commission, detection, apprehension, adjudication. Security intelligence operations are much more open-ended. The emphasis is on investigation, analysis, and the formulation of intelligence.[12]

---

12 Report of the Special Committee of the Senate on the Canadian Security Intelligence Service, *Delicate Balance: A Security Intelligence Service in a Democratic Society* (Ottawa: Supply and Services Canada, 1983), p. 6.

These oft-cited comments[13] defined the role of intelligence with an emphasis on secrecy and without discussion about when legitimate needs for secrecy might have to yield to the imperatives of disclosure in order to prevent and prosecute crimes affecting Canada's security.

The Supreme Court of Canada recently cited the Special Senate Committee's analysis, but appropriately warned that "…[t]he division of work between CSIS and the RCMP in the investigation of terrorist activities is tending to become less clear than the authors of [reports, including the Senate report] seem to have originally envisioned."[14]

Even in 1984, the need for CSIS to convey some information to the RCMP should have been apparent. For example, CSIS officers are not peace officers with law enforcement powers. If CSIS discovered evidence about a crime, that information would have to be conveyed to the police, who could then make arrests and lay charges. The immediate and continuing problem was the discretion vested in CSIS that allowed it to withhold information from the police. This would allow CSIS to continue a secret intelligence investigation in the hope of obtaining further information or catching more important targets. The refusal to pass on the information, however, meant that the "small fry" might not come to the attention of law enforcement and might therefore never be prosecuted.

In the immediate aftermath of revelations of wrongdoing by the RCMP Security Service during the 1970s, including unnecessary surveillance of political parties and dissenters, and after the subsequent creation of a civilian intelligence agency without law enforcement powers, greater emphasis was placed on defining differences between the RCMP and CSIS[15] than on the need for cooperation and sharing of information between the agencies. Nevertheless, the *CSIS Act* and the *Security Offences Act* contemplated and required cooperation between CSIS and

---

13 At the 2003 John Tait Memorial Lecture, Ward Elcock, then Director of CSIS, stated: "Law enforcement is generally reactive; it essentially takes place after the commission of a distinct criminal offence. Police officers are results-oriented, in the sense that they seek prosecution of wrong doers. They work on a 'closed' system of limits defined by the Criminal Code, other statutes and the courts. Within that framework, they often tend to operate in a highly decentralized mode. Police construct a chain of evidence that is gathered and used to support criminal convictions in trials where witnesses are legally obliged to testify. Trials are public events that receive considerable publicity. Security intelligence work is, by contrast, preventive and information-oriented. At its best, it occurs before violent events occur, in order to equip police and other authorities to deal with them. Information is gathered from people who are not compelled by law to divulge it. Intelligence officers have a much less clearly defined role, which works best in a highly centralized management structure. They are interested in the linkages and associations of people who may never commit a criminal act -- people who consort with others who may be a direct threat to the interests of the state.": "Appearance by Ward Elcock, Director, Canadian Intelligence Security Service, at the Canadian Association for Security and Intelligence Studies Conference," October 16-18, 2003, Vancouver, BC - "The John Tait Memorial Lecture," online: Canadian Security Intelligence Service <http://www.csis-scrs.gc.ca/nwsrm/spchs/spch17102003-eng.asp> (accessed July 29, 2009).

14 *Charkaoui v. Canada (Citizenship and Immigration)*, 2008 SCC 38, [2008] 2 S.C.R. 326 at para. 26.

15 Wark Paper on Intelligence-Law Enforcement Nexus, p. 150; Jean-Paul Brodeur, "The Royal Canadian Mounted Police and the Canadian Security Intelligence Service: A Comparison Between Occupational and Organizational Cultures" in Vol. 1 of Research Studies: Threat Assessment RCMP/CSIS Co-operation, pp. 193-196 [Brodeur Paper on Comparison Between RCMP and CSIS].

the RCMP with respect to crimes, such as the bombing of Air India Flight 182, that also constituted threats to the security of Canada.[16]

4.2 Section 12 of the *CSIS Act*, the Collection and Retention of Intelligence and the Implications of *Charkaoui v. Canada*

Section 12 is the cornerstone of the *CSIS Act*. This section governs the work of CSIS in collecting intelligence about threats to the security of Canada and in retaining and analyzing that intelligence. It also imposes duties on CSIS to provide the Government of Canada with reports and advice about security threats. Section 12 states:

> The Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada.

Issues relating to the collection and retention of intelligence were central to the Air India investigations and will be central to future terrorism investigations by CSIS. For this reason, the Commission examined these issues in detail.

4.2.1 The Destruction of Intelligence in the Air India Investigation

CSIS officials have justified the erasure of the Parmar Tapes as being a requirement of the collection and retention provisions of section 12 of the *CSIS Act*. In turn, the erasure of most of the tapes resulted in a concession by the Crown and in a finding by the trial judge in the Malik and Bagri trial that CSIS had violated section 7 of the *Charter* and engaged in unacceptable negligence in not retaining the material.[17] The Hon. Bob Rae described the tape erasures as

---

16 Kent Roach, "The Unique Challenges of Terrorism Prosecutions: Towards a Workable Relation Between Intelligence and Evidence" in Vol. 4 of Research Studies: The Unique Challenges of Terrorism Prosecutions, pp. 26-27 [Roach Paper on Terrorism Prosecutions].

17 *R. v. Malik*, *Bagri and Reyat*, 2002 BCSC 864 at paras. 7, 12. See also *R. v. Malik and Bagri*, 2004 BCSC 554, 119 C.R.R. (2d) 39 at paras. 19, 22.

"problematic," and as justifying a further and full examination of the relationship between intelligence and evidence.[18]

Reid Morden, a former head of CSIS, has been amongst the most ardent defenders of the propriety of the erasure of the tapes. In an interview carried by the CBC in 1987, he argued that "…the tapes of course are destroyed, not as a…bureaucratic procedure, where there's a matter of policy because we have to be very careful in terms of section 12 of our Act, that we collect information which is strictly necessary to an ongoing investigation."[19] When asked about this statement while he was testifying before the Commission, Morden said:

> Now, out of [the McDonald Commission] comes the *CSIS Act* and within the *CSIS Act*, I think the very important provision of Article 12, which enjoins the service to collect, only to the degree strictly necessary, the information. And from that I think grows the policy that says you collected – you're not collecting evidence, you're collecting information which can be turned into intelligence. If it doesn't appear to meet the test of Article 12 then this should be destroyed as opposed to being retained, as it had been previously.[20]

The content of the destroyed Parmar intercepts has long been the source of much controversy. In reviewing the matter, the Commission has concluded that, given the interpretation of the *CSIS Act* by Reid Morden, CSIS might be excused for tape erasures that occurred before the terrorist attacks on Flight 182 and at Narita, but that CSIS was wrong to continue to erase tapes after those events.

---

18 Bob Rae observed: "Justice Josephson noted that the destruction of these tapes was 'unacceptable negligence.' SIRC concluded in 1992 that the destruction of the tape erasure had no material impact on the RCMP investigation. This is a not a view shared by the RCMP, made clear in the memos of February 9th and 16th, 1996, written by Gary Bass, Assistant Commissioner of the RCMP and lead investigator into the Air India disaster since 1996. The erasure of the tapes is particularly problematic in light of the landmark decision of the Supreme Court of Canada in R. v. Stinchcombe, which held that the Crown has a responsibility to disclose all relevant evidence to the defence even if it has no plans to rely on such evidence at trial. Justice Josephson held that all remaining information in the possession of CSIS is subject to disclosure by the Crown in accordance with the standards set out in Stinchcombe. Accordingly, CSIS information should not have been withheld from the accused. The defence argument in the trial of Malik and Bagri was that erased tapes might have produced information that could exonerate their clients. For that reason alone, the tapes should never have been destroyed. The issue of the relationship between CSIS and the RCMP that was before Justice Josephson highlights the concerns about the connections between intelligence, the destruction of evidence, required disclosure and admissible evidence. It is clear that the relationship between these institutions and the interplay between intelligence and evidence requires further review": *Lessons to be Learned: The report of the Honourable Bob Rae, Independent Advisor to the Minister of Public Safety and Emergency Preparedness, on outstanding questions with respect to the bombing of Air India Flight 182* (Ottawa: Air India Review Secretariat, 2005), pp. 16-17 [*Lessons to be Learned*]. [Footnotes in original have been omitted.]

19 Inquiry Transcript, vol. 46, September 17, 2007, p. 5516, transcribing "The vanishing trail," Narr. Brian Stewart, *The Journal*, CBC (December 14, 1987), 11:45-12:47, online: CBC Digital Archives <http://archives.cbc.ca/society/crime_justice/clips/5691/> (accesed July 29, 2009). See Testimony of Reid Morden, vol. 88, December 4, 2007, pp. 11429-11430, commenting on his statements in the CBC interview.

20 Testimony of Reid Morden, vol. 88, December 4, 2007, p. 11430.

It is self-evident that the understanding of a given threat to national security evolves over time. It is rarely the case that one can fully appreciate a potential threat upon an initial assessment of information. It follows that retaining intelligence is necessary to allow for re-evaluation and analysis. As RCMP Deputy Commissioner Gary Bass noted:

> The erasure of the tapes is important for reasons beyond what occurred in the Air India case. I believe that the policy governing CSIS tape handling (which is essentially unchanged as I understand it) is seriously flawed and has potential to cause problems in future [counterterrorism investigations]. Anyone with experience in wiretap investigations understands that initial transcripts and translations can be notoriously unreliable. For one thing many intercepts, audio room or car bugs, in particular, require a huge use of time and resources to produce accurate transcripts. Secondly, the value of some intercepts early in an investigation cannot be properly interpreted or assessed until other "key" intercepts are made at some point later on. A policy requiring the destruction of tapes within 30 days is fraught with problems and should be adjusted to reflect the reality of conducting effective criminal prosecutions in today's reality of disclosure. The ruling in the Air India case in this respect will surely be held out to be "fair warning" in this respect in future similar fact situations.[21]

The O'Connor Commission stressed the importance of accuracy and precision in intelligence.[22] The Supreme Court of Canada has recognized that retention of raw intelligence can help ensure the accuracy and precision of intelligence.[23] Yet CSIS routinely destroyed information that it had lawfully acquired because of a prevailing view that it was to retain only what was strictly necessary.

The particulars of the retention policy varied over the years and the policy contained internal conflicts at times. However, it is clear that CSIS employed a policy of systematic destruction of intercepted communications where it could not identify or appreciate the relevance of the information.

The destruction policy applied not only to wiretaps, but also to original notes and working papers. Again, this had serious adverse consequences for the prosecution in the Malik and Bagri trial.[24] In his judgment, Justice Josephson noted the testimony of a CSIS agent at the trial that at meetings with a key witness he "…took careful notes, writing down what she said verbatim or his best efforts at summarizing what she said. From these notes he created a number of

---

21 Exhibit CAA1007: Gary Bass, Royal Canadian Mounted Police Briefing Note to the Commissioner, p. 3. See also Testimony of Gary Bass, vol. 87, December 3, 2008, pp. 11274-11276.

22 *Report of the Events Relating to Maher Arar: Analysis and Recommendations*, p. 114.

23 *Charkaoui v. Canada* (Citizenship and Immigration), 2008 SCC 38, [2008] 2 S.C.R. 326 at paras. 39-42.

24 *R. v. Mailk and Bagri*, 2005 BCSC 350.

internal reports which were filed as exhibits at trial. His handwritten notes from those meetings were destroyed as a matter of policy, with the exception of five pages of notes from their meeting on October 29, 1997."[25] Justice Josephson noted further that the CSIS agent stressed "…that he had not prepared his reports with the expectation they would be used in court" and that, while he attempted to summarize and report the interviews as accurately as possible, he was selective in what he included and he used his own language and not that of the critical witness.[26]

A second CSIS agent interviewed another key witness, Ms. E, but did not take contemporaneous notes. He "…did not attempt to track Ms. E's language in his reports since they were being prepared for intelligence, not evidentiary, purposes."[27] Justice Josephson found that the destruction of taped conversations with Ms. E constituted "unacceptable negligence" that violated section 7 of the *Charter*.[28] He also found that the promise that Ms. E's statements would remain confidential, and hence could not be subject to challenge, increased the potential of a credibility issue.[29] The incomplete nature of the reports also raised questions about their reliability.[30]

4.2.2 Interpreting Section 12 of the *CSIS Act*

As of the time of the Commission hearings, CSIS interpreted section 12 of the *CSIS Act* as requiring only that information that was "strictly necessary" be retained. The official position of CSIS was well-stated by Andrew Ellis, CSIS Director General of the Toronto Region, when he testified that "…[w]e must be guided by the *CSIS Act*, and the *CSIS Act* says we will retain information that is strictly necessary. And we use that as the guidepost constantly to determine what is retained and what is not retained."[31]

There is reason to question the correctness of this interpretation. The phrase "to the extent that it is strictly necessary" qualifies the term "collect" in section 12. The phrase does *not* qualify the terms "analyse" or "retain."[32] Once information is properly collected, CSIS has separate obligations to analyze and retain information, and there is no requirement that this be done only to the extent that it is strictly necessary. Indeed, it makes little sense to require analysis and retention only to the extent that is "strictly necessary."

Clearly, the retention of information can involve privacy interests. One concern that led to the formation of CSIS was the finding that the RCMP Security Service held files on many Canadians, including those involved in legitimate political and

25 2005 BCSC 350 at para. 386.
26 2005 BCSC 350 at para. 386.
27 2005 BCSC 350 at para. 999.
28 *R. v. Malik and Bagri*, 2004 BCSC 554, 119 C.R.R. (2d) 39.
29 *R. v. Malik and Bagri*, 2005 BCSC 350 at paras. 1128, 1232.
30 2005 BCSC 350 at para. 1132.
31 Testimony of Andrew Ellis, vol. 82, November 23, 2007, p. 10537.
32 Roach Paper on Terrorism Prosecutions, p. 116.

labour activity and democratic dissent. Nevertheless, "…the primary invasion of privacy is the collection of the information in the first place."[33] This collection should occur only to the extent that it is strictly necessary to investigate "… activities that may on reasonable grounds be suspected of constituting threats to the security of Canada." The Supreme Court of Canada recently paraphrased section 12 as follows: "…CSIS must acquire information to the extent that it is strictly necessary in order to carry out its mandate, and must then analyse and retain relevant information and intelligence."[34]

In any event, CSIS altered its policy in the wake of 9/11. Jim Judd, head of CSIS when he testified, stated that CSIS retains more information today, especially material that is shared with the RCMP. Judd stated that "…with respect to terrorist investigations, certainly over the last number of years, post-9/11, the practice has been for a long retention."[35] Longer retention periods are justified, especially in terrorism investigations, but they also indicate that section 12 of the *CSIS Act* should never have served as a barrier to the retention of properly collected intelligence such as the Parmar wiretaps and notes of interviews with key witnesses.

4.2.3 The Supreme Court of Canada's Interpretation of Section 12 of the CSIS Act in *Charkaoui*

The interpretation of section 12 employed by CSIS over the years can no longer be sustained in light of the Supreme Court of Canada's 2008 ruling in *Charkaoui v. Canada*,[36] a case decided after the Commission's hearings ended. The Court was critical of a CSIS policy that had interpreted section 12 to require the retention of operational notes only when "…information contained in the notes may be crucial to the investigation of an unlawful act of a serious nature and employees may require their notes to refresh their memories prior to recounting the facts of an event."[37] The Court concluded that this policy was inconsistent with the plain language of section 12. The Court found further that the policy was inconsistent with the obligations under section 7 of the *Charter* to retain material for possible disclosure to a person held under a security certificate issued under Canada's immigration laws.

The Court concluded that "…as a result of s. 12 of the *CSIS Act*, and for practical reasons, CSIS officers must retain their operational notes when conducting investigations that are not of a general nature. Whenever CSIS conducts an investigation that targets a particular individual or group, it may have to pass

---

33 Roach adds that "…care should be taken to ensure that only information that satisfies the standard of being 'strictly necessary' is retained. There were legitimate concerns, especially at the time that CSIS was created, that it not retain information that had not been collected under the rigourous standard of strict necessity": Roach Paper on Terrorism Prosecutions, p. 116.

34 *Charkaoui v. Canada* (Citizenship and Immigration), 2008 SCC 38, [2008] 2 S.C.R. 326 at para. 38.

35 Testimony of Luc Portelance, vol. 88, December 4, 2007, pp. 11496-11497; Testimony of Jim Judd, vol. 90, December 6, 2007, p. 11875.

36 *Charkaout v. Canada (Citizenship and Immigration)*, 2008 SCC 38, [2008] 2 S.C.R. 326.

37 The CSIS policy was identified as OPS-217, with this particular wording found at para. 3.5, as quoted in *Charkaout v. Canada (Citizenship and Immigration*), 2008 SCC 38, [2008] 2 S.C.R. 326 at para. 35.

the information on to external authorities or to a court."[38] The Court reasoned that the reference to "intelligence" in section 12 "…should not be limited to the summaries prepared by officers" because original notes "…will be a better source of information, *and of evidence*…."[39] The Court added that "…[t]here is no question that original notes and recordings are the *best evidence*."[40] The Court rejected the idea that section 12 justifies the destruction of properly obtained intelligence:

> Nothing in this provision requires CSIS to destroy the information it collects. Rather, in our view, s. 12 of the *CSIS Act* demands that it retain its operational notes. To paraphrase s. 12, CSIS must acquire information to the extent that it is strictly necessary in order to carry out its mandate, and must then analyse and retain relevant information and intelligence.[41]

This unanimous decision of the Supreme Court discredits the policy that resulted in the destruction of the Parmar Tapes.

In future, once intelligence is properly collected under section 12, it should be retained. In particular, the original notes and recordings should be retained — presumably until the information has become of no value — since they constitute the best source of information and the best source of evidence.

The retention of the original intelligence does not necessarily mean that the intelligence will be used in subsequent legal proceedings or disclosed to the target of the investigation. It will still be necessary to determine that a criminal prosecution is in the public interest. Even once a prosecution is commenced, the disclosure of intelligence is by no means automatic. The Attorney General of Canada can apply for a non-disclosure order on the basis that the harms that disclosure would cause to national security, national defence or international relations would be greater than the harms of non-disclosure.[42]

The Supreme Court's decision in *Charkaoui* has affirmed that the proper interpretation of section 12 of the *CSIS Act* requires the retention of properly collected intelligence, in part because it may also constitute the "best evidence."[43] The Court's decision, concluding that interview notes about a particular person should be retained under section 12, is also consistent with Justice Josephson's decision that CSIS had a duty in the Air India investigation to retain such notes.[44]

---

38 2008 SCC 38, [2008] 2 S.C.R. 326 at para. 43.
39 2008 SCC 38, [2008] 2 S.C.R. 326 at para. 39 [Emphasis added].
40 2008 SCC 38, [2008] 2 S.C.R. 326 at para. 49 [Emphasis added].
41 2008 SCC 38, [2008] 2 S.C.R. 326 at para. 38.
42 *Canada Evidence Act*, R.S.C. 1985, c. C-5, s.38 [*Canada Evidence Act*]. This is discussed further in Chapter VII.
43 2008 SCC 38, [2008] 2 S.C.R. 326 at paras. 39, 49.
44 *R. v. Malik and Bagri*, 2004 BCSC 554, 119 C.R.R. (2d) 39.

It would be a mistake to limit the interpretation of section 12 in *Charkaoui* to the immigration context. The Supreme Court noted that the RCMP receives much information in national security investigations from CSIS[45] and that CSIS, under section 19 of the *CSIS Act*, "…may disclose information to police services, to the Attorney General of Canada, to the Attorney General of a province, to the Minister of Foreign Affairs and to the Minister of National Defence."[46] The Court also discussed the importance of retaining original raw intelligence about disputes that may arise over the denial of security clearances.[47] The Court articulated a general principle that was not limited to immigration security certificates:

> In our view, as a result of s. 12 of the *CSIS Act*, and for practical reasons, CSIS officers must retain their operational notes when conducting investigations that are not of a general nature. Whenever CSIS conducts an investigation that targets a particular individual or group, it may have to pass the information on to external authorities or to a court.[48]

The Supreme Court's decision in *Charkaoui* does not directly address the retention of information derived from wiretaps authorized under section 21 of the *CSIS Act*. Nevertheless, if interview notes of potential witnesses should be retained in part because they could provide the best evidence, it is only common sense that wiretaps of suspects who might potentially be accused of terrorism should also be retained.

4.2.4 The Need for New CSIS Policies on Retention of Intelligence

The Supreme Court ruling in *Charkaoui* also benefits CSIS. A lengthy retention period can allow CSIS to better understand and analyze intercepted communications to determine the extent of a terrorist threat, without the pressure to destroy the intelligence prematurely.

For practical and privacy reasons, a policy should be established to prevent information obtained by CSIS from being retained indefinitely. Nevertheless, there is a need for a lengthy retention period. Many national security investigations, like the Air India investigation, continue for much longer than ordinary criminal investigations. Information collected at one point may take on new significance years later and be needed for intelligence or evidentiary purposes. For example, an individual at the periphery of one investigation may become more central in a subsequent investigation. The circumstances of individuals targeted in one investigation may change and they might become potential informers years later. Canada's foreign partners may take an interest in a target only when that target moves away from Canada. Such possibilities all favour a lengthy retention period.

---

45 2008 SCC 38, [2008] 2 S.C.R. 326 at para. 27.
46 2008 SCC 38, [2008] 2 S.C.R. 326 at para. 47.
47 2008 SCC 38, [2008] 2 S.C.R. 326 at para. 39.
48 2008 SCC 38, [2008] 2 S.C.R. 326 at para. 43.

If information has been properly collected – that is, if the collection is strictly necessary for an investigation of activities that may on reasonable grounds be suspected of constituting threats to Canada's security – the information should be retained. Evidence was presented to the Commission that CSIS now retains intelligence for longer periods in some counterterrorism investigations. These lengthier retention periods should become the norm.

In general, CSIS information about specific targets could be discarded if the Director of CSIS certifies that the information no longer relates to activities that may on reasonable grounds be suspected of constituting threats to the security of Canada. This standard has the virtue of being derived from section 12 of the *CSIS Act* as clarified by the Supreme Court in *Charkaoui*. It may also be appropriate to retain some information to allow archival research. However, adequate measures must be taken to protect the privacy of individuals.

As for the precise retention period, that is best left to CSIS to consider in consultation with other stakeholders. However, a period of 25 years does not strike the Commission as unreasonable or problematic.

The idea that a civilian security agency would retain information that may be of assistance to the police is not radical or dangerous. British legislation has been amended to recognize that both its domestic and foreign security intelligence agencies should be prepared to disclose information for the purpose of preventing, detecting and prosecuting serious crime.[49]

CSIS policies also need to reflect the Supreme Court's position in *Charkaoui* that intelligence collected in relation to particular individuals and groups be retained. It may also be time to revisit Article 21 of the 2006 Memorandum of Understanding (MOU) between the RCMP and CSIS. The MOU states that "… both parties recognize that the CSIS does not normally collect information or intelligence for evidentiary purposes."[50]

Another possibility would be to amend section 12. However, the section has been clarified by a unanimous decision of the Supreme Court. Amending the section might re-introduce uncertainty about the extent of the obligation of CSIS to retain intelligence. In addition, the current section 12 reflects a delicate balance between security and privacy interests by allowing CSIS to collect information and intelligence only "…to the extent that it is strictly necessary" and only with respect to "…activities that may on reasonable grounds be suspected of constituting threats to the security of Canada."

---

49 *Security Services Act* 1989 (UK), 1989, c. 5, s. 2(2)(a); *Intelligence Services Act* 1994 (UK), 1994, c. 13, s. 2(2)(a).

50 Public Production 1374: 2006 RCMP/CSIS MOU, Art. 21(a).

4.2.5 Conditions for the Collection of Intelligence

If intelligence is to be retained longer in accordance with the reasoning in *Charkaoui*, it becomes important to revisit when intelligence should be collected in the first place. Section 12 of the *CSIS Act* was drafted following revelations that the RCMP Security Service had engaged in unnecessary investigations of a variety of dissenters, including those involved in various political parties such as the Parti Québécois and the New Democratic Party.[51] In response, the McDonald Commission stressed that the activities of the civilian intelligence agency it proposed should be limited by a carefully defined mandate. In addition, the collection of intelligence should be governed by the principle that "…the investigative means used must be proportionate to the gravity of the threat posed and the probability of its occurrence."[52]

The McDonald Commission's principles of a carefully defined mandate and proportionality in investigations and in the collection of intelligence are reflected in section 12. The section provides, in part, that CSIS "…shall collect, by investigation or otherwise, to the extent that it is strictly necessary… intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada."

The Supreme Court in *Charkaoui* stressed that "…CSIS must acquire information to the extent that it is strictly necessary in order to carry out its mandate."[53] This means that intelligence should not be collected unless it relates to activities that may on reasonable grounds be suspected of constituting threats to Canada's security. The reasonable suspicion standard requires that there be an objective and articulable basis for the investigation that relates to threats to the security of Canada as defined in the *CSIS Act*. Even when a reasonable suspicion is present, CSIS should observe principles of proportionality and collect intelligence only to the extent that it is "strictly necessary."

What is "strictly necessary" will inevitably depend on the investigation, including the severity and imminence of the threat and countervailing concerns such as privacy and the freedom to engage in lawful democratic dissent.

Some information that is collected through electronic or human sources might not be related to activities that may on reasonable grounds be suspected of constituting threats to Canada's security, or its collection might not be strictly necessary for an investigation of such threats. For example, an electronic or human source may reveal information relating to private misdeeds or lawful activities. Such activities may pose no security threat. In other cases, activities may be peripherally relevant to an investigation of threats to the security of Canada, but should not be the focus of an investigation because of the adverse impact on privacy.

---

51 Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Freedom and Security under the Law*, Second Report - vol. 1 (Ottawa: Supply and Services Canada, 1981), pp. 341-358 [*Freedom and Security under the Law*].

52 *Freedom and Security under the Law*, Second Report - vol. 1, p. 513.

53 2003 SCC 38, [2008] 2 S.C.R. 326 at para. 39.

If such information has been inadvertently collected, it should not be retained.[54] The retention obligation in section 12 of the *CSIS Act* should apply only to information that has been collected in accordance with section 12. In making this judgment, however, CSIS should be careful not to destroy information that could later assist either the investigation or individuals targeted by the investigation. For example, information about a private misdeed should be retained if it could potentially support a target's alibi.

In the 2008 *Charkaoui* decision, the Supreme Court of Canada articulated a principle that distinguished targeted from general investigations. The rationale for this distinction seems to be the common sense observation that a targeted investigation, focused on a specific individual or group, is likely to have more serious consequences for individuals than a general investigation into phenomena, such as extremism or foreign countries, which may affect Canada's national security. This rationale is reflected in the Court's statement that "… [w]henever CSIS conducts an investigation that targets a particular individual or group, it may have to pass the information on to external authorities or to a court."[55] If the information is passed on to external authorities, such as the police, foreign agencies or the courts, the likelihood of serious consequences for an individual increases. For example, intelligence about a specific individual could be used to deny that person a security clearance. It could also trigger a criminal investigation or detention in a foreign country.

Once an investigation targets a particular individual or group, intelligence collected during that investigation should be retained even if the intelligence is about individuals who are not the targets of the investigation. Although the analogy is not perfect because he was examining a criminal investigation, Commissioner O'Connor found that it was reasonable for the RCMP to investigate Maher Arar because he was associated with the target of the Project A-O Canada investigation.[56] If the RCMP acted reasonably in collecting information about Arar, then it is even more likely that CSIS, in exercising its broader security intelligence mandate, would also be justified in collecting information about a person who associated with the target of its investigation in suspicious circumstances. The distinction between targets and associated persons, especially in a terrorism investigation, is not always obvious.

---

54 The Inspector General of CSIS in 1996 described the approach as follows: "CSIS is expected to employ an objective standard, namely demonstrable grounds for suspicion and to ensure that it documents its grounds." He added that the documentation must indicate that "…techniques of investigation that penetrate areas of privacy [were] used only when justified by the severity and imminence of the threat to national security": Craig Forcese, *National Security Law: Canadian Practice in International Perspective* (Toronto: Irwin Law, 2008), p. 83.

55 2008 SCC 38, [2008] 2 S.C.R. 326 at para. 43.

56 Report of the Events Relating to Maher Arar: Analysis and Recommendations, p. 18. Project A-O Canada was created in the aftermath of the 9/11 attacks to carry out an investigation into the activities of Abdullah Almalki. It was also charged with investigating any leads about the threat of a second wave of attacks. The project's investigation subsequently expanded to include new information that it received about other individuals and activities: Report of the Events Relating to Maher Arar: Analysis and Recommendations, p. 16.

The collection and retention of intelligence should, to the extent possible, be done with attention to the relevance, accuracy and reliability of the intelligence collected, as well as to its effects on human rights and privacy. Intelligence collected in accordance with the mandate of CSIS and in compliance with section 12 of the *CSIS Act* should be retained for two reasons: it ensures the fair treatment of individuals in the form of precise, accurate and verified intelligence and it has potential value in legitimate national security investigations. The retention of intelligence in the form in which it was collected will help to ensure that the analysis produced by investigators is accurate and precise.

As well, the retention of original data is considered good practice in many fields, and CSIS should follow suit. Scientists and social scientists keep their raw data even though their ultimate work product is analysis and interpretation of the data. CSIS should retain raw data to allow investigators and those who may review the work of investigators, such as supervisors, SIRC and, sometimes, judges, to test the accuracy, fairness and reliability of the final intelligence product.

4.3 Privacy Issues

The destruction of tapes and original notes in the Air India investigation and the Supreme Court's recent ruling in *Charkaoui* both serve to underline the need to retain raw intelligence. However, this should not be taken as a justification to return to the pre-CSIS days where the RCMP Security Service kept files on individuals involved in legitimate political or religious activities and engaged in intrusive investigations of those individuals.

Increased and lengthier retention of intelligence by CSIS raises privacy concerns. Stanley Cohen, for example, has argued that intelligence dossiers can contain "…a range of information, including much that is unsifted or unfiltered, as well as innuendo, hearsay and speculation," and that the amassing of detailed information leads to "…dossier building and the creation of generalized suspect lists."[57] These are legitimate concerns.

The *CSIS Act* already imposes restraints to prevent this. Section 12 requires CSIS to collect intelligence about "activities that may on reasonable grounds be suspected of constituting threats to the security of Canada." "Threats to the security of Canada" are carefully defined in section 2 of the Act. As well, section 12 requires meeting the investigative threshold of "reasonable suspicion" before collection is permitted. The concept of reasonable suspicion is recognized in other areas of law and it is similar to that used by the police when commencing investigations.[58] In addition, CSIS must respect principles of proportionality; intelligence should be collected only to the extent that it is "strictly necessary." With these constraints on collection in place, the retention of the intelligence collected should not be problematic.

---

57 Stanley A. Cohen, *Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril* (Markham: LexisNexis, 2005), p. 404 [Cohen, Privacy, Crime and Terror].

58 Final Submissions of the Attorney General of Canada, Vol. I, para. 494.

In some cases, retaining the original intelligence will protect those who later become the targets of enforcement and other actions, by revealing inaccuracies in the CSIS analysis or improprieties in the collection of the intelligence. In other cases, retaining the original intelligence will help protect the security of Canadians, by providing leads and revealing connections that were not apparent when the intelligence was collected and first analyzed. In all cases, retention of the original intelligence will help ensure that the important analytical work done by CSIS is accurate and precise because the work can be tested against the raw data.

CSIS search powers, including the power to engage in electronic surveillance, must meet a higher standard than that set out in section 12 governing the collection, analysis and retention of information. To obtain the authority to search, CSIS investigators must *believe*, not merely suspect, on reasonable grounds, that a warrant is required to investigate a threat to the security of Canada. In addition, section 21 requires that other investigative procedures have failed, would be unlikely to succeed or that the matter is urgent.

There is also a second layer of privacy protection. CSIS is subject to extensive review of its activities, including its policies and practices about retaining and sharing intelligence. The Inspector General of CSIS must inform the Minister of Public Safety if CSIS engages in operational activities that are not authorized under the *CSIS Act* or that contravene ministerial directives. Ministerial directives, for example, restrict investigations in sensitive sectors and investigations which involve unreasonable or unnecessary use by CSIS of its powers.[59] In addition, the Inspector General's Certificates are referred to the Security Intelligence Review Committee (SIRC), which reviews the performance of CSIS and hears complaints against it.[60] In both its reviews and in its hearings of complaints from people denied security clearances, SIRC should be concerned with the accuracy and reliability of the intelligence that CSIS shares with other agencies and that leads CSIS to act. SIRC's reviews should provide some protection against the misuse of intelligence files that contain untested data.

The *Privacy Act*[61] provides additional protections. Any sharing of intelligence would have to be justified under one of the limited exceptions, which include consistent use, law enforcement and the public interest.[62] The Office of the Privacy Commissioner may also audit and review even the "exempt banks" of data held by CSIS.

---

59 *CSIS Act*, s. 33.
60 *CSIS Act*, ss. 34-55.
61 R.S.C. 1985, c. P-21.
62 Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (Ottawa: Public Works and Government Services Canada, 2006), pp. 286, 433-436 [*A New Review Mechanism for the RCMP's National Security Activities*]; *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin* (Ottawa: Public Works and Government Services Canada, 2008), pp. 82, 92, 393-395, 434-435 [*Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin*].

Finally, concerns about privacy are mitigated by the limited uses CSIS can make of the intelligence that it retains. Intelligence held by CSIS is generally kept secret. If the intelligence is distributed to other agencies, it should, as Justice O'Connor has recommended, be screened for relevance, reliability, accuracy and privacy concerns, and appropriate restrictions or caveats on its subsequent distribution should be attached.[63]

Recommendation 9:

In compliance with the 2008 Supreme Court of Canada decision in *Charkaoui*, CSIS should retain intelligence that has been properly gathered during an investigation of threats to national security under section 12 of the *CSIS Act*. CSIS should destroy such intelligence after 25 years or a period determined by Parliament, but only if the Director of CSIS certifies that it is no longer relevant.

4.4 Section 19 of the *CSIS Act* and the Distribution of Intelligence

Section 19(2)(a) of the *CSIS Act* constituted an important recognition that the intelligence CSIS collected should in some cases be shared with police and prosecutors. This sharing would occur if the intelligence would be relevant to the investigation and prosecution of crimes such as terrorism that also constituted a threat to the security of Canada. Section 19(2)(a) recognizes that the mandate of CSIS to investigate threats to the security of Canada overlaps with the mandate of police and prosecutors to investigate and prosecute serious crimes such as terrorism and espionage.

Consistent with the emphasis on secrecy in the activities of a security intelligence agency, section 19(1) provides a general rule that "…information obtained in the performance of the duties and functions of the Service under this Act shall not be disclosed…." This general rule is, however, qualified by section 19(2)(a):

> The Service *may* disclose information referred to in subsection (1) for the purposes of the performance of its duties and functions under this Act or the administration or enforcement of this Act or as required by any other law and may also disclose such information,
>
> a. where the information may be used in the investigation or prosecution of an alleged contravention of any law of Canada or a province, to a peace officer having jurisdiction to investigate the alleged contravention and to the Attorney General of Canada and the Attorney General of the province in which proceedings in respect of the alleged contravention may be taken. [Emphasis added]

63 Report of the Events Relating to Maher Arar: Analysis and Recommendations, p. 343.

Sections 19(2)(b)(c) and (d) contemplate disclosure of CSIS information to various ministers, including the Minister of Foreign Affairs and the Minister of National Defence.

The problem with these provisions is that they give CSIS the sole discretion to pass information to any other agency. In the exercise of its discretion, CSIS can decide not to disclose information about a crime.

4.4.1 CSIS Discretion under Section 19(2)(a) Not to Share Relevant Information with the Police

There is evidence that the discretion in section 19(2)(a) was used, especially in the early stages of the post-bombing investigation, to thwart full cooperation by CSIS with the RCMP. When testifying before the Commission, Jacques Jodoin, Director General of Communications Intelligence and Warrants, confirmed that he had written a memorandum stating that, "…in accordance with the legal advice we have received on s. 19(2)(a), we cannot give RCMP direct access to transcripts [of the Parmar wiretaps]; we can only provide them investigational leads…."[64] Merv Grierson, who had been both head of Counter-Intelligence and Deputy Director of Counter Terrorism in the BC Region, testified that there was a "continual stand-off" between CSIS and the RCMP about section 19(2)(a) during the investigation.[65]

James ("Jim") Warren, a retired CSIS officer, even testified that he objected to a liaison program between the RCMP and CSIS on the basis that it would remove the Director's discretion not to turn information over to the police.[66] Although the liaison program was sensibly introduced over such objections, the fact that such objections were even made demonstrates the fear at CSIS of being pulled into the world of law enforcement, disclosure and the courts.[67]

Jack Hooper, a former Deputy Director of CSIS, testified that he believed that he would be "…failing to meet the expectations of the legislators and removing from the Director the discretionary power that was accorded to him"[68] if he provided the RCMP with raw information during an investigation. On the other hand, former RCMP Commissioner

Giuliano Zaccardelli testified about the problems that a lack of disclosure caused:

---

64 Testimony of Jacques Jodoin, vol. 49, September 20, 2007, p. 6056.
65 Testimony of Merv Grierson, vol. 75, November 14, 2007, pp. 9474-9475.
66 Testimony of James Warren, vol. 48, September 19, 2007, p. 5909.
67 For an argument that the lack of CSIS cooperation in the immediate post-bombing period was related more to internal rivalries than to any essential differences at that time between CSIS as a security intelligence agency and the RCMP as a police force, see Brodeur Paper on Comparison of RCMP and CSIS, pp. 191, 202-203.
68 Testimony of Jack Hooper, vol. 50, September 21, 2007, p. 6221.

> When you look at the actual legislation [*CSIS Act*] and the interpretation that's been given to that legislation, that's where we have the problem. The legislation and the way it is interpreted has not been – has not enabled the agencies to effectively and efficiently carry out their mandates when the exchange of information is inhibited by what, at times, is very narrow interpretations of the various sections which allow for the flow of information or the retention of certain information as happens sometimes, in particularly with CSIS….
>
> That word ["may"] has caused – is really at the centre of the problem because if you interpret "may" in a narrow way then you have the problems that were created – that have historically been at the centre of the issue.[69]

4.4.2 Rationales for CSIS Discretion Not to Give the Police Relevant Information

It is important to understand why CSIS might want discretion to withhold information that would be of use to police and prosecutors. The following concerns, among others, could justify its support for the discretion not to share relevant information with the police:

- concerns about revealing covert agents and sources of CSIS;
- concerns about maintaining the secrecy of the information that CSIS shares, particularly in subsequent prosecutions; and
- concerns about disrupting ongoing security intelligence investigations.

CSIS has a statutory obligation not to disclose intelligence that could reveal confidential sources of information or the identity of CSIS employees engaged in covert operational activities. However, section 18(2) provides that a person may disclose such information "…in the circumstances described in any of paragraphs 19(2)(a) to (d)." Thus, the protection for confidential sources and covert agents set out in section 18 is not a legal impediment to disclosing information for law enforcement and prosecution purposes. Still, CSIS could have concerns that disclosing information would increase the risk that the identity of secret human sources or covert agents could be disclosed. There is some evidence that CSIS gives its human sources "…absolute promises that their identity will be protected" and that such practices are believed to be necessary in the recruitment of sources and in the discharge by CSIS of its duty to collect intelligence about security threats.[70]

---

69 Testimony of Giuliano Zaccardelli, vol. 86, November 30, 2007, pp. 11022-11024.
70 *Harkat (Re)*, 2009 FC 204 at para. 31.

CSIS possibly might also want to withhold relevant secret information from law enforcement officials because of a concern that such officials may not have the requisite security clearances, training or facilities to ensure the security of the information. Some secret information, if inadvertently disclosed, could place the life of a human source at risk or jeopardize an ongoing investigation. These are legitimate concerns, but they have largely been addressed through measures to ensure adequate security procedures for INSETs and other national security investigators. Police officers also often have experience with secret human sources – those protected by police informer privilege.

Another possible reason for CSIS to want to withhold information from the police is the concern that a police arrest could disrupt an ongoing and highly important intelligence investigation. Luc Portelance, Deputy Director of Operations at CSIS, testified that the discretion not to disclose information "…provides us all of the latitude that we need" to protect "…some ongoing investigations whereby there's absolutely no need to inform the RCMP. It could be in the counter-intelligence domain, it could be in the counter-proliferation domain…. So you would never want to take away from us, I think, the discretion that we have."[71] Assistant Commissioner Mike McDonell of the RCMP agreed with Portelance that, given the breadth of the CSIS mandate, the discretion not to disclose information for law enforcement purposes should be retained.

McDonell stressed the "…current environment of openness and of discussion"[72] that informs the exercise of discretion by CSIS not to disclose relevant information to the police. Meetings between the RCMP and CSIS to prevent conflicts during their respective investigations or to address those conflicts were discussed in Chapter II. This positive environment could deteriorate as people retire or move on, and as the sense of urgency in post 9/11 reforms that stressed greater cooperation and integration dissipates. As Hooper testified, "…at the end of the day the solution must be a legal solution, a legislative solution, not a relationship solution."[73]

The risk that disclosure of CSIS information to the police could compromise ongoing security intelligence investigations is reduced by the requirement of the consent of the federal or provincial Attorney General to commence proceedings for terrorism offences.[74] As well, proceedings with respect to the *Security of Information Act* cannot be commenced without the consent of the Attorney General of Canada.[75] In both cases, the principle of police independence, which has been interpreted to preserve the freedom of police officers to exercise their discretion to lay charges and make arrests, has been qualified in the national security context.

---

71 Testimony of Luc Portelance, vol. 88, December 4, 2007, pp. 11516-11517.
72 Testimony of Mike McDonnell, vol. 95, December 13, 2007, p. 12663.
73 Testimony of Jack Hooper, vol. 50, September 21, 2007, pp. 6247-6248.
74 *Criminal Code*, R.S.C. 1985, c. C-46, s. 83.24 [*Criminal Code*] ; *A New Review Mechanism for the RCMP's National Security Activities*, p. 460. See also Chapter III.
75 *Security of Information Act*, R.S.C. 1985, c. O-5, s. 24.

The most compelling reason for the discretion vested in CSIS not to disclose information to police or prosecutors is the concern that once information is in the hands of the police or prosecutors, it might eventually be disclosed in court. The Security Intelligence Review Committee, in a series of reports in 1998 and 1999, described concerns within CSIS "…that all CSIS intelligence disclosures, regardless of whether they would be entered for evidentiary purposes by the Crown, are subject to disclosure. Any passage of information, whether an oral disclosure or in a formal advisory letter, could expose CSIS investigations. This means that even information that is provided during joint discussions on investigations or that is provided as an investigative lead is at risk."[76] The SIRC reports emphasized how the broad obligations articulated in *Stinchcombe*[77] to disclose all relevant information had adversely affected information sharing between the RCMP and CSIS.

When CSIS gives information to the RCMP, this entails a risk that the information will be disclosed later in legal proceedings. It does not in every case mean that the information will be disclosed. The police investigation may not produce sufficient evidence to lay criminal charges. Even if there is sufficient evidence, the Attorney General might not consent to the laying of terrorism charges.[78] Even if charges are laid, the intelligence may not meet the relevance standard that would require its disclosure to the accused. Even if the intelligence is relevant and should be disclosed, the Attorney General of Canada can seek a non-disclosure order under section 38 of the *Canada Evidence Act*[79] on the grounds that the harms of disclosure to national security outweigh the need for disclosure. Even if a court concludes that intelligence must be disclosed, the Attorney General of Canada can issue a certificate under section 38.13 that prevents disclosure on the basis that it was received from or in relation to a foreign entity or relates to national defence or national security. Finally, the Attorney General of Canada can stay a terrorism prosecution to avoid disclosure.

The list of means of protecting intelligence from disclosure described above means that CSIS should not equate sharing information with the police to the inevitable disclosure of the information to the accused or the public in a prosecution. There is a risk of disclosure, but CSIS perceives the risk to be greater than it is in fact. This distorted perception makes CSIS unnecessarily reticent to share information with the RCMP.

4.4.3 Submissions on CSIS Discretion to Share Information with the Police

The Air India Victims' Families Association submitted that the discretion of CSIS to disclose information should be abolished. In short, they request that the "may" in section 19(2) of the *CSIS Act* be changed to "shall."[80] CSIS would then be

76 SIRC Study 1998-04, p. 9.
77 *R. v. Stinchcombe*, [1991] 3 S.C.R. 326.
78 *Criminal Code*, s. 83.24.
79 R.S.C. 1985, c. C-5.
80 *Where is Justice?* AIVFA Final Written Submission, Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, February 29, 2008, p. 97 [AIVFA Final Written Submission].

required to disclose information to police and prosecutors that it currently has *discretion* to disclose or withhold.

The Attorney General of Canada did not recommend eliminating this discretion. The Attorney General described the CSIS discretion as a key part of the legislative scheme and warned that if the RCMP had full access to CSIS information, "… innocent people could be drawn into a criminal investigation solely on the basis of a link to a CSIS target."[81]

Several witnesses testified about section 19. Former RCMP Commissioner Zaccardelli emphasized the importance of "effective and efficient movement" of information given the current threat environment:

> …I realize that the Air India disaster was one of the greatest tragedies that has ever taken place in the world; the most important, or the most serious crime that ever took place in Canada. That was one event but what we face today is a repeated series of threats, therefore, the need to have that information flow becomes even more crucial and it must flow in a timely manner and it cannot be given a restrictive interpretation because the risks are so high. The higher the risk the more attempt must be made to give a more liberal interpretation to the release of information.[82]

Zaccardelli's comments underline that the risk that intelligence shared by CSIS with the RCMP will subsequently be disclosed is not the only or necessarily the most important risk. Another is that a refusal to share information will prevent law enforcement from making arrests or from taking other actions that could prevent an act of terrorism such as the bombing of Air India Flight 182.

4.4.4 The Commission's Proposed Approach to Information Sharing

The preferable way to reconcile the competing interests in sharing information with the police and in maintaining the secrecy of information is to require CSIS to provide information that could be relevant and of use in criminal terrorism investigations either to the relevant police and prosecutors or to the NSA.

The *status quo* is not acceptable because it allows CSIS to decide unilaterally for the Government of Canada when relevant information should or should not be shared with other agencies. The *status quo* entails the risk that police and prosecutors may not receive important information that could assist them in terrorism investigations and prosecutions. Moreover, it precludes anyone in the Government of Canada outside CSIS from learning about the information. Although CSIS is ultimately accountable to the Minister of Public Safety and is

---

81 Final Submissions of the Attorney General of Canada, Vol. I, para. 335.
82 Testimony of Giuliano Zaccardelli, vol. 86, November 30, 2007, pp. 11024, 11030.

subject to review by the Inspector General and by SIRC, it is unlikely that any of these can effectively supervise how CSIS exercises its discretion under section 19(2)(a) not to disclose relevant information.

CSIS should not have a residual discretion to withhold highly sensitive intelligence. Although the current relationship between the RCMP and CSIS is apparently good and is resulting in improved sharing of information by CSIS, this relationship could deteriorate, and CSIS might use its discretion to limit the sharing of information that should be shared in the public interest.

The remote possibility of disclosure to an accused at some unknown future time should not justify preventing CSIS from sharing relevant information with police to allow the police to take actions that may help prevent an act of terrorism. To allow concerns about possible eventual disclosure effectively to prevent CSIS from sharing information with the police is to allow the tail to wag the dog. The first priority should be to ensure the sharing of information that is necessary to protect the safety of Canadians.

At the same time, there would be problems if, as recommended by the Air India Victims' Families Association, the "may" in section 19(2) were simply amended to "shall." That would require CSIS to share relevant information with the police in all cases. As discussed, CSIS may have legitimate reasons to oppose sharing information about sensitive investigations and secret sources and methods. Relevant information shared with the police might be subject to broad constitutional obligations to disclose the information to the accused. Although steps could be taken to prevent such disclosure of sensitive intelligence, there would be no certainty that they would be successful. Even the risk of disclosure could jeopardize CSIS investigations and its relations with sources and allied agencies. It is also possible that CSIS could adopt restrictive interpretations of what information could be relevant and of use in criminal investigations if it was simply required to share all such information with the police.

Section 19(2)(a) of the *CSIS Act* should be amended to require that CSIS "shall" disclose information that "…may be used in the investigation or prosecution" of an offence. However, CSIS should still have some discretion – whether to provide such information to police and prosecutors and accept the risk of subsequent disclosure, or to provide the information to the NSA. The NSA would then decide, in the public interest, if and when the information should be provided to the police or to another agency. The NSA would have the power at any time to require CSIS to give the information to police, prosecutors or to any other agency.

CSIS should have this obligation to report only for information about "…threats to the security of Canada" as defined in section 2 of the Act.[83] This would limit the mandatory reporting requirement to CSIS terrorism investigations, where the balance between the competing demands for secrecy and disclosure is the most delicate.

These changes would give statutory recognition to the enhanced role of the NSA proposed in Chapter II.

This two-track approach, in which CSIS would either provide relevant information directly to the police or to the NSA, would allow CSIS to continue its current practice of increasing the flow of information about its counterterrorism investigations to the RCMP. Many new terrorism offences were created in 2001 and, as *Charkaoui* articulated, increased obligations have been imposed on CSIS to retain intelligence relating to particular individuals. For these reasons, CSIS will likely continue to provide increasing amounts of information about its terrorism investigations to the RCMP. This is a positive trend, but both the O'Connor[84] and Iacobucci[85] reports stressed the care that must be taken with shared information. The RCMP must relate information received from CSIS to the RCMP's criminal law mandate and must take steps to ensure the accuracy, reliability and relevance of the information that the RCMP receives.

The Commission understands the concerns of CSIS about the possibility of the information it shares with the RCMP being disclosed to the defence. The Commission also acknowledges concerns that some CSIS intelligence investigations are so sensitive that there are dangers in simply providing information about them to the police and prosecutors who, under the *Charter*, are subject to broad disclosure obligations.[86] Even a slight risk that sensitive intelligence could be disclosed publicly could adversely affect CSIS and, potentially, the safety of Canadians. For these reasons, CSIS should have the option of providing information that may be relevant to terrorism investigations and prosecutions to the NSA instead of to the relevant policing and prosecutorial authorities.

The Commission cannot predict how much information CSIS will share with the RCMP or with the NSA under this proposed regime. The Commission heard evidence that CSIS already is passing more counterterrorism information to the RCMP than it did previously. Although he did not support an amendment that

---

83 This mandate relates to international and domestic terrorism defined as "…threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state." It would be best to define CSIS's new mandatory reporting obligations in terms of its own mandate rather than with respect to what for CSIS will be the less familiar concepts of either terrorist activities or terrorist offences as defined in the *Criminal Code*.

84 *Report of the Events Relating to Maher Arar: Analysis and Recommendations*, p. 103.

85 *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin*, p. 69.

86 *R. v. Stinchcombe*, [1991] 3 S.C.R. 326; *R. v. McNeil*, 2009 SCC 3. See Chapter V for more discussion of the scope of these disclosure obligations.

would eliminate the CSIS discretion not to disclose relevant intelligence, Luc Portelance of CSIS testified that present-day integration of CSIS and the RCMP was such that the current discretion to share information under section 19 applied almost as if it was obligatory.[87] Henry Jensen, a former RCMP Deputy Commissioner of Operations, also testified that an MOU between the RCMP and CSIS had effectively already changed the "may disclose" in section 19(2) to "shall disclose."[88]

CSIS is likely to become more willing to provide information directly to the RCMP as CSIS becomes more comfortable with the safeguards in the legal system to prevent the further disclosure of intelligence. Introducing a Director of Terrorism Prosecutions, as proposed earlier, will probably increase the level of comfort within CSIS, because there will be expert advice available from the Director about the many remedies that are available to prevent the further disclosure of intelligence that CSIS provides to the police.

4.4.5 The Role of the National Security Advisor in Sharing CSIS Information

On receiving information from CSIS, the NSA would decide what to do with the information. CSIS would be permitted to express fully to the NSA its views about possible risks in disclosing the intelligence to the RCMP or in using the intelligence in some other way, such as border control or immigration. CSIS would not, however, have a veto on sharing the information with the RCMP, unlike the current situation, where CSIS has discretion under section 19(2)(a) of the *CSIS Act* whether or not to share the information. Under the new proposal, the NSA would have the ultimate authority to decide whether CSIS information should be shared with the RCMP. The NSA would be expected to act in the public interest in each case and would not be beholden to any interest of CSIS in withholding information from other agencies. Equally, the NSA would not be bound to serve any interest of the RCMP in having the information provided to it to facilitate an investigation or subsequent prosecution.

In some cases, the NSA might conclude that national security investigations should continue without providing CSIS information to police and prosecutors. In such cases it would be prudent for the NSA to be briefed regularly about the national security investigation. At some point, the NSA might decide that it would be appropriate to pass information to police, prosecutors or other agencies in Canada or abroad. The NSA could be selective, deciding that some CSIS information should be given to border officials or to those responsible for aviation security, but not to the RCMP, at that time.

If the NSA determined that the CSIS information should be made available to police and prosecutors, the NSA would provide the information to them. The principles of police and prosecutorial independence and discretion would,

87 Testimony of Luc Portelance, vol. 88, December 4, 2007, p. 11515.
88 Testimony of Henry Jensen, vol. 18, March 7, 2007, pp. 1650-1651.

however, prevent the NSA from compelling the police to commence an investigation or prosecutors to lay charges.

CSIS should be prepared to explain to the NSA any decision it makes to pass terrorism-related information to the NSA instead of to the police. Although it is impossible to predict what percentage of information will be passed from CSIS to the RCMP or to the NSA (and that percentage may change over time), it can be expected that the NSA will receive information in the most difficult and sensitive cases. This would place a special obligation on the NSA to stay informed about those cases and to seek appropriate advice about them.

Information that CSIS provides to the NSA should be subject to a new statutory national security privilege. It would be patterned after the existing privilege under section 39 of the *Canada Evidence Act* that shields information submitted to assist with Cabinet deliberations.[89] The new privilege would apply to documents prepared for review by the NSA and to the NSA's deliberations. The details of the privilege are discussed in Chapter VI.

The new privilege might at first encourage CSIS to disclose more intelligence to the NSA than to the RCMP. Nevertheless, the NSA could provide that intelligence to the RCMP at any time. Once CSIS information was passed on to the RCMP, the new national security privilege would no longer apply.

Recommendation 10:

The CSIS Act should be amended to reflect the enhanced role proposed for the National Security Advisor and to provide for greater sharing of information with other agencies.

Section 19(2)(a) of the CSIS Act should be amended to require CSIS to report information that may be used in an investigation or prosecution of an offence either to the relevant policing or prosecutorial authorities or to the National Security Advisor.

If the National Security Advisor receives security threat information from CSIS, he or she should have the authority, at any time, to provide the information to the relevant policing or prosecutorial authorities or to other relevant officials with a view to minimizing the terrorist threat. The National Security Advisor should make decisions about whether intelligence should be disclosed only after considering the competing demands for disclosure and secrecy. In every case, the decision should be made in the public interest, which may differ from the immediate interests of the agencies involved.

Intelligence prepared to assist the National Security Advisor in his or her deliberations, and the deliberations themselves, should be protected by a new

89 *Canada Evidence Act*, s. 39.

national security privilege. The privilege would be a class privilege similar to that protecting information submitted to assist with Cabinet deliberations.

4.5 Culture Change within CSIS: Beyond "We Don't Collect Evidence"

Earlier sections discussed the need for two significant reforms: longer retention by CSIS of the intelligence it collects, and an amendment to section 19(2)(a) of the *CSIS Act* to remove the current CSIS discretion to withhold relevant information from other agencies. However, these reforms alone are not sufficient to ensure continuing improvement in the relationship between CSIS and the RCMP. CSIS must take into account evidentiary and disclosure standards in its counterterrorism investigations. CSIS must move beyond the mantra that it does not collect evidence.

Warren testified that, during the time of the Air India investigation, disclosure was seen as the equivalent of "…handing the keys to the church to the devil."[90] The attitude from that era must not be allowed to persist if CSIS is to work effectively in a threat environment that may require arrests and prosecutions in terrorism cases. The frustrations of police and prosecutors, because of resistance from CSIS to meeting evidential and disclosure standards in its investigations, were well and forcefully expressed by James Jardine, the lead prosecutor in the Reyat case. His words, written in 1991, deserve being repeated:

> There is little value in gathering intelligence for intelligence purposes….It is my view that CSIS should consider the development of the service to include the capacity to pass information, intelligence, and evidence to the appropriate police agency in a form which will allow the police agency to use the 'information' in evidence gathering for the prosecution. To do that the Service must come to grips with the thorny issues created by the disclosure requirements for full answer and defence in criminal prosecutions.[91]

Jardine went on to suggest that this required CSIS to accept that its personnel would at times testify in criminal proceedings and would have to preserve evidence for court purposes.[92] It took 17 years, but the 2008 Supreme Court decision in *Charkaoui*[93] vindicated the concerns expressed by Jardine.

Supreme Court decisions, however, do not change attitudes or standard operating policies overnight. CSIS needs to ensure that it truly accepts the

90 Testimony of James Warren, vol. 48, September 19, 2007, p. 5839.
91 Public Production 10005936: James Jardine, Q.C., "The Use of Security Intelligence in Canadian Criminal Proceedings," Speaking Notes for an October 3, 1991 Seminar at Ottawa, p. 36 [Jardine Notes on Use of Security Intelligence in Canadian Criminal Proceedings].
92 Jardine Notes on Use of Security Intelligence in Canadian Criminal Proceedings.
93 2008 SCC 38, [2008] 2 S.C.R. 326.

evidential and disclosure implications of its counterterrorism investigations. This does not mean that CSIS should become a police force, or what is pejoratively called a "cheap cop shop." CSIS must continue to collect intelligence to inform the Government of Canada about threats to national security. That remains the mandate of CSIS. However, CSIS should no longer resist or ignore the reality that its counterterrorism investigations will often overlap with criminal investigations and that some intelligence may have to be used as evidence.

Most of the emphasis in the early years of CSIS was placed on differentiating the activities of the new agency from those of the RCMP. Various SIRC reports that reviewed the work of CSIS affirmed the idea that CSIS did not collect evidence. SIRC also suggested that the RCMP's frustration flowed from a misunderstanding of the statutory mandate of CSIS. For example, SIRC's public report on the Air India investigation commented that:

> … [a]s the investigation progressed, RCMP officials felt it necessary to examine CSIS files on certain Sikh extremist targets in more detail. CSIS, whose mandate it is to collect intelligence and not evidence, was at first reluctant to expose its files, and by extension its methods and sources, for any evidentiary use by the RCMP. Lengthy negotiations took place between the two agencies, but eventually the RCMP investigators were allowed access to the files subject to some mutually agreed conditions on the subsequent use of the information.
>
> Overall, we found no evidence that access to available CSIS information relevant to the RCMP investigation of the disaster was unreasonably denied to the Force.[94]

SIRC returned in 1998 to the theme that CSIS did not collect evidence, when SIRC commented that:

> …some RCMP investigators see some CSIS information as evidence that is vital to a successful prosecution, but which can be denied to them by caveats placed on the information by CSIS or that, even if used, will be subject to the Service invoking sections 37 and 38 of the Canada Evidence Act, an action that could seriously impede the RCMP's case. The Service view is that it does not collect evidence. This possible misunderstanding on the part of some RCMP investigators may result in certain CSIS information/intelligence being

94 *Security Intelligence Review Committee Annual Report 1991-92*, p. 10, online: Security Intelligence Review Committee <http://www.sirc-csars.gc.ca/pdfs/ar_1991-1992-eng.pdf> (accessed July 29, 2009).

> treated as though it were evidence but which might not stand up to Court scrutiny because it had not been collected to evidentiary standards. [95]

SIRC noted that some RCMP officers complained that CSIS was overly protective of its human sources, but it concluded that withholding information to protect third party information, human sources and methods of operation "…is consistent with Service policy," and was clearly stated in the terms of a Memorandum of Understanding.[96] The message sent to CSIS was that the frustrations of police and prosecutors were caused simply by misunderstanding the CSIS mandate.

The widely-held view that CSIS did not collect evidence also meant that legal requirements for disclosure were viewed with suspicion and alarm within CSIS. Professor Wesley Wark commented on the 1991 *Stinchcombe* decision, which required the disclosure to the accused of relevant information possessed by the Crown. According to Wark, *Stinchcombe* had "…the effect of further cementing CSIS's self-image as an intelligence service that collected information for national security purposes, not evidence. It potentially deepened the RCMP's difficulties in sustaining the flow of intelligence, deemed worthwhile as investigative leads, from CSIS."[97]

Police and prosecutors were frustrated by CSIS attitudes. The frustration within the RCMP made that agency more reluctant to work with CSIS. It spawned what has been described earlier in this volume as a philosophy of the RCMP that can be summarized as "the less information we receive from CSIS, the better." SIRC noted that RCMP O Division had reduced its requests for disclosure letters from CSIS by 90 per cent, in large part "…because the *Stinchcombe* decision had effectively turned CSIS information into what was described as a 'poison pill' when a related prosecution was initiated."[98] The reluctance of the RCMP to obtain CSIS intelligence was accompanied by an increasingly strained relationship between the two agencies.

MI5, the British equivalent of CSIS, recognizes the need at times for intelligence to be disclosed and then to be used as evidence. The MI5 website provides the following statement: "The increased involvement of the Service in criminal proceedings means that, when planning and carrying out intelligence investigations that may lead to a prosecution, we keep in mind the requirements of both the law of evidence and the duty of disclosure."[99] At the same time, the legal system has assisted MI5 by allowing agents to testify anonymously and behind screens, although they are subject to cross-examination. Similarly, MI5 has explained how trial judges can make non-disclosure orders in cases where

---

95 SIRC Study 1998-04, p. 9.
96 SIRC Study 1998-04, p. 6.
97 Wark Paper on Intelligence-Law Enforcement Nexus, p. 165.
98 SIRC Study 1998-04, p. 7.
99 Security Service MI5 (United Kingdom), "Evidence and Disclosure," online: Security Service MI5 (United Kingdom) <http://www.mi5.gov.uk/output/evidence-and-disclosure.html> (accessed July 29, 2009) [MI5, "Evidence and Disclosure"].

"…disclosure would cause real damage to the public interest by, for example, compromising the identity of an agent or a sensitive investigative technique…. [I]t is the courts, not the Service or the Government, that ultimately decide what must be disclosed in a particular case. If a claim is accepted, the judge will continue to keep the decision under review throughout the proceedings."[100] The British example is instructive. It demonstrates how security intelligence agencies and the legal system can work together to better manage the relationship between intelligence that can be kept secret and evidence that must be disclosed to ensure a fair prosecution.[101]

The balance between intelligence and evidence was altered by the *Anti-terrorism Act*. The Act created many new criminal offences that may be committed by acts of support, facilitation and participation in a terrorist group – activities that may occur long before any overt terrorist act. The Hon. Bob Rae raised the following valid concerns in his report:

> If an agency believes that its mission does not include law enforcement, it should hardly be surprising that its agents do not believe they are in the business of collecting evidence for use in a trial. But this misses the point that in an age where terrorism and its ancillary activities are clearly crimes, the surveillance of potentially violent behaviour may ultimately be connected to law enforcement.[102]

RCMP Deputy Commissioner Gary Bass testified about RCMP concerns that CSIS is still not sufficiently attuned to the needs of law enforcement. He stated that "…there is something inherently wrong with the process now where… it's accepted that CSIS is not in the business of gathering evidence, yet they're expected to make an assessment on evidence to decide whether or not they retain tapes.…[I]t just doesn't make sense to me."[103]

Appropriate CSIS officials should receive adequate training and legal advice about the law regarding disclosure of intelligence and the relevance of intelligence to terrorism prosecutions. This is necessary to complement the policy changes proposed in this chapter about section 12 of the *CSIS Act* and the removal of the current discretion vested in CSIS not to share information for law enforcement or prosecution purposes under section 19(2)(a).

The proposed Director of Terrorism Prosecutions could play a key role in educating CSIS about the law surrounding disclosure. The Director could also provide continuity of legal advice about disclosure matters, something that

---

100 MI5, "Evidence and Disclosure."

101 Wiretap evidence, however, is not generally admissible in British prosecutions. The issue of the use of CSIS wiretap warrants as evidence and the appropriate balance between CSIS and *Criminal Code* wiretap warrants is discussed later in this chapter.

102 *Lessons to be Learned*, p. 23.

103 Testimony of Gary Bass, vol. 87, December 3, 2007, p. 11284.

has not always been available and that may have led to exaggerated fears that intelligence shared with the RCMP would have to be disclosed to the accused. It is important for CSIS to appreciate that the law has a robust regime to protect intelligence from disclosure.

CSIS standard operating procedures must change to accommodate disclosure requirements. In its submissions to the Commission, the Canadian Bar Association cited several cases where CSIS continued to destroy notes taken from key sources and notes taken at other meetings. The Association pointed out that, "…[f]or a police force to direct [that] such policies be followed would clearly be a gross and deliberate violation of an accused's right to full answer and defence. It appears CSIS accepts this as routine and justified by the interests of national security."[104] The Supreme Court's subsequent decision in *Charkaoui*[105] confirmed that CSIS had destroyed interview notes that should have been retained and concluded that CSIS retention policies were inadequate.

There are signs that the leadership at CSIS is aware of the trends towards greater disclosure of intelligence collected in counterterrorism investigations. In a speech given in April 2008, Jim Judd, the Director of CSIS at the time, referred to the "judicialization" of intelligence, where intelligence was increasingly becoming involved in the legal process. He commented:

> One of the consequences of recent trends in anti-terrorism actions has been a growing number of criminal prosecutions that have often had at their genesis, information collected by intelligence and not law enforcement agencies.
>
> This in turn has increasingly drawn intelligence agencies in some jurisdictions into some interesting and important debates on a range of legal issues such as disclosure, evidentiary standards, and the testimony of intelligence personnel in criminal prosecutions.
>
> While not startling or novel issues for the legal or police communities, these do have significant potential implications and consequences for the conduct of intelligence operations. In some instances, they have also stimulated some interesting debates over the boundary lines between law enforcement agencies and intelligence services.[106]

---

104 Canadian Bar Association, Submission to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, April 2007, p. 18.

105 2008 SCC 38, [2008] 2 S.C.R. 326.

106 "Remarks by Jim Judd, Director of CSIS, at the Global Futures Forum Conference in Vancouver" (April 15, 2008), online: <http://www.csis-scrs.gc.ca/nwsrm/spchs/spch15042008-eng.asp> (accessed July 29, 2009) [Judd Remarks at Global Futures Forum Conference].

Judd also observed that a variety of factors, including legal proceedings, were driving a debate about "…what is legitimately secret and what is not," and that these changes "…raise the issue as to whether or not existing legislative regimes are still current."[107]

Yet CSIS appeared resistant to change earlier. In a 2006 speech, Judd commented that, "… [u]nlike the police, we do not collect evidence per se (or collect information to evidentiary standards) to prosecute and secure convictions in court proceedings."[108] In his testimony before the Commission, Judd stated that "…the notion that there is a significant overlap between the two mandates of the organizations in respect of terrorism is greatly overestimated or overblown." He stated in support of his position that there were only three cases since 9/11 where a CSIS investigation coincided with a police investigation that resulted in charges.[109] Although he characterized this as minimal overlap, it is significant in light of the few cases in which terrorism charges have been laid in Canada since 9/11. In many cases where terrorism prosecutions have been launched, CSIS has conducted a previous or a contemporaneous investigation.

Judd's comments that CSIS does not collect intelligence to evidentiary standards, combined with the Supreme Court's decision in *Charkaoui*[110] about the inadequacy of CSIS retention policies, demonstrate that CSIS still has not fully accepted that intelligence collected in counterterrorism investigations will at times have to be disclosed and used as evidence in terrorism prosecutions. Securing acceptance by CSIS is especially important, given that counterterrorism investigations now consume most of the resources of CSIS.

CSIS witnesses who testified before the Commission appeared to assume that preventing disclosure and preserving the anonymity of sources was the only means to protect such vulnerable persons. Hooper testified that "…the identification of our sources in the public domain is anathema to the Service to the extent that it really, at the end of the day, attenuates our ability to effectively do our jobs."[111] The concern about the ability of CSIS to do the job of supplying intelligence also explained why, according to Hooper, "…we are rather religious in terms of protecting the identity of assets, whether they be technical or human or any other form."[112]

The desire of CSIS to protect vulnerable human sources is understandable. Nevertheless, the collection of intelligence is not a goal in and of itself. The collection of intelligence should assist in preventing terrorism. This will

---

107 Judd Remarks at Global Futures Forum Conference.

108 "Transparency and Intelligence, Notes for Remarks at Royal Canadian Military Institute (RCMI) Toronto, Ontario, Jim Judd, Director, Canadian Security Intelligence Service" (September 28, 2006), online: Canadian Security Intelligence Service <http://www.csis-scrs.gc.ca//nwsrm/spchs/spch28092006-eng.asp> (accessed July 29, 2009).

109 Testimony of Jim Judd, vol. 90, December 6, 2007, p. 11851.

110 2008 SCC 38, [2008] 2 S.C.R. 326.

111 Testimony of Jack Hooper, vol. 50, September 21, 2007, p. 6217.

112 Testimony of Jack Hooper, vol. 50, September 21, 2007, p. 6217.

sometimes require intelligence provided by secret sources to be disclosed to police and possibly lead to the source's identity being revealed during a prosecution.

The legal system is far from powerless to protect human sources. As will be discussed in subsequent chapters, identifying information about some police informers can be protected by the police informer privilege. In addition, prosecutors can seek a variety of non-disclosure orders from the courts.

Although they need to be improved and can impose hardships, witness protection programs are also available. As Professor Jean-Paul Brodeur observed in a paper written for the Commission, there is no reason for CSIS to be unfamiliar with witness protection programs. CSIS should recognize that its ultimate objective is to protect Canadians and that collecting secret intelligence and using secret human sources are simply means to that end. With respect to the Air India bombing, Brodeur observed that "…giving priority to the protection of one's informants over solving this monstrous crime is tantamount to losing sight of the point that infiltration is a means towards the end of protecting the nation and its people. Infiltration and the protection of informants is not an end for its own sake." [113]

Both the *CSIS Act* and the culture of CSIS must change to respond to the challenges presented by the investigation of terrorism as both a threat to the security of Canada and as a crime. It is no longer appropriate for CSIS to continue to rely on the historical notion that it does not collect evidence or that there is very little overlap between its counterterrorism work and that done by the police. The time has come for a more contemporary approach to the counterterrorism effort.

4.6 Culture Change in the RCMP: Beyond "The Less Information We Receive from CSIS, the Better"

The RCMP must also change. A number of representatives of the RCMP testified about a philosophy of "the less information we receive from CSIS, the better." The precise expression that was sometimes used in testimony before the Commission was "less is more," but this expression should best be left where it originated – as a description of simplicity of architectural and furniture design – not in the police vocabulary as a description of attitudes about receiving intelligence from CSIS.

---

113 Brodeur Paper on Comparison of RCMP and CSIS, p. 209. Brodeur explains that "[T]he police usually make short-term use of their informants, perform sting operations with their assistance, and have no qualms about calling informants to testify in court, since governments have witness protection programs. Security intelligence agencies such as CSIS infrequently mount sting operations, since they have no law enforcement mandate; they try to use sources for as long as possible and go to great lengths to protect their identity": pp. 207-208. He then relates CSIS practices of long-term running of informants to an attempt at long-term curtailment of a group which can give rise to "a means over ends" approach.

RCMP Commissioner Elliott testified that "…sometimes it's better for us not to know things, and I think that's part of the dilemma. How much do we need to know in order to take action, as opposed to more detailed information that might then give rise to a situation where that balancing would have to be made with respect to whether information, on the one hand, should be disclosed or it should not be disclosed, and that might be determined on whether or not a prosecution could succeed or proceed."[114] RCMP Assistant Commissioner McDonnell testified about how he could supplement "hints" from CSIS with his own investigations in order to avoid the dilemmas presented by disclosure of CSIS information.[115]

The philosophy of "the less information we receive from CSIS, the better" is far from ideal. Former RCMP Commissioner Zaccardelli placed his finger on the problem when he observed that "…[w]e've been concentrating [more] on guarding the information for our own silos rather than working on how we can guard it and still share it at the same time."[116]

This philosophy also assumes that CSIS information will not be subject to disclosure demands if it is not passed to the RCMP. This assumption is incorrect. The Malik and Bagri prosecution provides an example of a court concluding that the close integration between CSIS and the RCMP in the investigation made CSIS subject to *Stinchcombe* disclosure obligations. Even if this ruling is ultimately not sustained by a higher court, CSIS will still be subject to demands by the accused to produce important information. This will be the case even if CSIS is classified as a third party that is not bound by *Stinchcombe* disclosure obligations.[117]

The accused may not in all cases be successful in obtaining disclosure of material held by CSIS. Where the accused is successful, the Attorney General of Canada can still claim privileges and seek non-disclosure orders to protect that material. Nevertheless, the real possibility of the accused obtaining disclosure of intelligence from CSIS suggests that the RCMP approach of avoiding the acquisition of intelligence from CSIS is not an effective or reliable means of protecting that intelligence from disclosure. It also deprives the RCMP of valuable information. Hence, the philosophy of "the less information we receive from CSIS, the better" must be abandoned.

Like CSIS, the RCMP needs to become more comfortable with the variety of instruments that can be used to protect intelligence from disclosure. The RCMP needs to become more sensitive to CSIS concerns about secrecy and about the responsibility of CSIS to collect intelligence about threats to the security of Canada. The RCMP and CSIS should both be able to obtain consistent legal advice about disclosure matters.

---

114 Testimony of William Elliott, vol. 90, December 6, 2007, p. 11814.
115 Testimony of Mike McDonell, vol. 95, December 13, 2007, pp. 12635.
116 Testimony of Giuliano Zaccardelli, vol. 86, November 30, 2007, p. 11037.
117 See the discussion of *R. v. O'Connor*, [1995] 4 S.C.R 411 and *R. v. McNeil*, 2009 SCC 3 in Chapter V.

The RCMP should continue to take the lead in counterterrorism investigations where there is evidence of criminality. As discussed earlier, the *Anti-terrorism Act* has moved ahead the point where criminality begins by creating offences relating to the financing and facilitation of terrorism and various forms of participation in terrorist groups, crimes which occur before the actual terrorist act.

CSIS should not destroy intelligence and, where possible, it should collect it to evidentiary standards. However, the police should remain the lead agency in collecting evidence for use in court. The police have the necessary experience and internal procedures to ensure that evidence is collected in a form that will make it admissible in court. An additional benefit of giving the lead role to the police is the ability of the police to disrupt terrorist plots, if necessary, through arrests and other enforcement actions.

Recommendation 11:

To the extent that it is practicable to do so, CSIS should conform to the requirements of the laws relating to evidence and disclosure when conducting its counterterrorism investigations in order to facilitate the use of intelligence in the criminal justice process.

4.7 Using CSIS Information in a Criminal Trial: Section 21 of the *CSIS Act*

Electronic surveillance and human sources are the two most important means of investigating terrorist plots. Section 21 of the *CSIS Act* sets out a warrant regime that allows a designated judge of the Federal Court to grant a warrant to intercept communications, documents and other relevant information. To obtain a warrant, there must be reasonable grounds to believe that the search is required to allow CSIS to investigate a threat to the security of Canada or to perform its duties under section 16 of the Act.[118] In addition, the judge must be convinced that other investigative procedures are not practical.

The Attorney General of Canada submitted that section 21 of the *CSIS Act* contains the same "reasonable grounds" standards that are generally used in *Criminal Code* warrant applications. This statement is correct as far as it goes, but it does not go far enough.

The basis for a *Criminal Code* warrant application is that the affiant has reasonable grounds to believe that an offence has been, or will be, committed. An affiant applying for a section 21 warrant under the *CSIS Act* must only have a belief, on reasonable grounds, that a warrant is required to enable CSIS to investigate a threat to the security of Canada. The affiant does not need to

---

118 Section 16 authorizes CSIS in certain circumstances to collect information about foreign states and certain foreign individuals and corporations.

specify a reasonable belief that an offence has been, or will be, committed. The section 21 warrant could relate to someone reasonably suspected of being involved in a terrorist or other threat to the security of Canada, even if no offence is specified. For this reason, it is likely that a CSIS warrant will be less difficult to obtain than a *Criminal Code* warrant in the early stages of a terrorist conspiracy or plot.

There has been limited experience in criminal trials with the use of information obtained through section 21 warrants. In his testimony, the Hon. Bob Rae described this as the "intelligence-evidence conundrum": "…[H]ow do we get that information and evidence before a Judge without threatening or affecting the whole intelligence gathering operation that we have, which is, by its very nature, secretive…and sometimes relies on physical sources, like a wiretap, sometimes relies on information from a live source, from a human being, you know, the so-called 'humint' – human intelligence, and how do we make that transition" from intelligence to evidence?[119]

In the 1987 case of *Atwal*,[120] the Federal Court of Appeal, in a 2:1 judgment, held that the section 21 scheme was consistent with the right set out in section 8 of the *Charter* to be secure against unreasonable search or seizure. The majority noted that the Supreme Court of Canada, in *Hunter v. Southam*,[121] left open the possibility that the grounds for issuing a warrant in matters of national security could justify departures from the criminal law requirement of reasonable and probable grounds relating to an assertion that a crime has been or is about to be committed. Accordingly, the fact that the reasonable grounds requirement in section 21 of the *CSIS Act* related to an assertion that there was a threat to national security was, for the majority, sufficient to satisfy constitutional standards.

Although decided more than 20 years ago, *Atwal* remains the leading case. It provides authority for the proposition that, in appropriate cases, the government could introduce evidence from searches authorized under section 21 of the *CSIS Act*.

In its submissions to the Commission, the Criminal Lawyers' Association argued against the increased use of intelligence as evidence in criminal cases because of concerns about the reliability of intelligence and the lack of judicial review.[122] However, concerns about reliability do not apply to recorded conversations and seized tangible evidence. As for judicial review, the defence can argue that the admission of the product of a section 21 search would violate the *Charter*. While not a traditional form of judicial review, this is a form of adjudication of the merits of the warrant.

---

119 Testimony of Bob Rae, vol. 6, October 4, 2006, pp. 554-555.
120 *R. v. Atwal* (1987), 36 C.C.C. (3d) 161 (F.C.A.).
121 *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145.
122 Submissions of the Criminal Lawyers' Association, February 2008, pp. 13-33.

At present, an attempt to use material gathered under section 21 of the *CSIS Act* as evidence in a criminal trial comes at a price of having to make disclosure to the accused. That is, the state is required to disclose the affidavit used to obtain the warrant. The affidavit would generally contain much information about CSIS sources, methods and ongoing investigations.

However, disclosure would not be inevitable. The government could remove from the affidavit information that might reveal the identity of a confidential human source or covert agent. In addition, the Attorney General could apply for a non-disclosure order under the *Canada Evidence Act* on the grounds that the harms of disclosure to national security or another specified public interest are greater than the harms of non-disclosure to the accused.[123]

Disclosure to an accused of the sworn material used to obtain the CSIS wiretap warrant would, however, be required at present in a criminal trial. Any material deleted from the affidavit to protect secrets could not be relied upon to support the constitutionality of the warrant and search. An affidavit used to obtain a warrant could be so heavily edited, in order to protect secret intelligence, sources and methods, that it would no longer contain sufficient information to prove the legality or constitutionality of the warrant. That said, under present rules of evidence there is no impediment in a criminal trial to using the information obtained under a *CSIS Act* warrant.

As already indicated, electronic surveillance and human sources are vital tools to investigate terrorist plots such as the one to bomb Air India Flight 182. In some cases, wiretaps authorized under section 21 may reveal evidence about criminal conspiracies or about the new crimes that apply to the financing or facilitation of terrorist activities, participation in a terrorist group or instructing a person to carry out an activity for a terrorist group.

CSIS should retain the product of wiretaps because they provide the most accurate source of intelligence and, possibly, the best evidence. The interpretive notes of an analyst who has listened to the tapes are not good enough. There is another reason for retaining the product of the wiretap. The wiretap may need to be re-evaluated in light of changed circumstances, even where the wiretap is used solely for intelligence purposes.

4.7.1 The Important and Expanded Role of *Criminal Code* Electronic Surveillance in Terrorism Investigations

The *Anti-terrorism Act* created many new crimes relating to terrorist financing, facilitation and participation in a terrorist group. These crimes can be committed long before an overt act of terrorism and, therefore, make possible the much earlier use of warrants under Part VI of the Criminal Code as well as the more usual warrants under section 21 of the *CSIS Act*.

---

123 *R. v. Atwal* (1987), 36 C.C.C. (3d) 161 at 189-192 (F.C.A.).

The grounds for granting a *Criminal Code* warrant are different than those for granting a *CSIS Act* warrant. A *Criminal Code* warrant is authorized on the basis of reasonable grounds to conclude that a crime has been, is being or will be committed and that the intercept will provide evidence of that offence. A *CSIS Act* warrant is granted on the basis that there are reasonable grounds to believe that a warrant is required to enable CSIS to investigate a suspected threat to the security of Canada.

As a result of the 2001 *Anti-terrorism Act* amendments, warrants under Part VI of the *Criminal Code*, when the proper conditions are fulfilled, may have some advantages when compared to warrants under section 21 of the *CSIS Act*. Unlike the situation when seeking a warrant under section 21 of the *CSIS Act*,[124] there is no requirement with a *Criminal Code* warrant relating to a terrorism offence to establish that other investigative procedures such as surveillance, informers, undercover agents and regular search warrants would not be successful or practical.[125]

Both the duration of *Criminal Code* warrants and the permissible delays in notifying targets were significantly extended by the *Anti-terrorism Act*, making *Criminal Code* warrants a more useful tool for investigating possible terrorist offences. Like the *CSIS Act* warrants, *Criminal Code* warrants in support of a terrorism investigation can be valid for up to a year.[126] However, persons subject to a wiretap authorized under the *Criminal Code* must eventually be notified that their privacy has been invaded, although the *Criminal Code* permits delaying notification for up to three years in terrorism cases.[127] There is no notification requirement for those subject to a wiretap authorized under section 21 of the *CSIS Act*. Because notice to a target could affect the viability of an intelligence investigation which might very often continue for longer than three years, the notification requirement may often argue in favour of applying for a warrant under the *CSIS Act* instead of under the *Criminal Code*.

The access to Part VI warrants for investigations of the early stages of planned terrorism offences provide by the *Anti-terrorism Act* means that management-of-the-threat discussions between CSIS and the RCMP should take place earlier than has previously been the case. If such discussions lead to greater use of electronic surveillance under the *Criminal Code*, there will be a requirement for earlier and closer cooperation and coordination between the two agencies.

The important role of the joint RCMP/CSIS management team (JMT) was discussed in Chapter II. One function of the JMT should be a formal discussion of targeting decisions made by both CSIS and the RCMP in their counterterrorism investigations. During these discussions, there should be careful consideration of the comparative merits of seeking a *Criminal Code* or *CSIS Act* warrant.

---

124 *CSIS Act*, s. 21(2)(b).
125 *Criminal Code*, s. 186(1.1). Note that "terrorism offence" is defined in s. 2.
126 *Criminal Code*, s. 186.1.
127 *Criminal Code*, ss. 196(1), (5).

4.7.2 Electronic Surveillance Outside Canada

Because much terrorism has international elements, targets of Canadian counterterrorism investigations may frequently travel abroad. A decision of the Federal Court released after the Commission's public hearings concluded held that warrants cannot be granted under section 21 of the *CSIS Act* to authorize searches or electronic surveillance outside Canada. The case involved 10 individuals who were the targets of section 21 warrants and who, during the currency of the warrants, then left Canada.[128] In such circumstances, Canada must rely on a foreign agency to conduct surveillance. Although this arrangement sometimes works well, foreign agencies often will not have the same priorities or use the same methods as CSIS.

There are other options for the conduct of surveillance on suspects who leave Canada, such as a possible ministerial authorization under the *National Defence Act*[129] authorizing the Communications Security Establishment (CSE) to collect foreign intelligence through the global communications infrastructure.

Reliance upon CSE is not a satisfactory substitute to empowering CSIS. First, CSE is not permitted to conduct surveillance of Canadians. Second, it is doubtful that the regime would pass constitutional standards, since the electronic surveillance is conducted under a ministerial authorization not a warrant issued by a judge. Third, the *National Defence Act* requires that that private communications be retained only if they are essential to international affairs, defence or security.[130] This restriction will lead to the destruction of more raw intelligence than would be the case under the standard that applies to CSIS, as defined by the Supreme Court of Canada in *Charkaoui*.[131] For these reasons, reliance on CSE is not an adequate substitute for amending section 21 of the *CSIS Act* to permit surveillance abroad.

The Air India Victims Families Association expressed concern about a gap in coverage that may be created by the inability to conduct electronic surveillance of targets when they leave Canada.[132] This is undoubtedly true, but determining the appropriate solutions raises complex issues of international law, international cooperation and technical capacity that were not fully examined by the Commission as they were beyond its mandate. It is the Commission's view that the Government of Canada needs to address this issue in the near future. It seems preferable to integrate such surveillance activities into the CSIS mandate rather than to create a separate institution with a mandate to conduct investigations outside Canada.

---

128 *Canadian Security Intelligence Service Act* (Re), 2008 FC 301, 4 F.C.R. 230 at para. 54.
129 R.S.C. 1985, c. N-5, s. 273.65.
130 *National Defence Act*, R.S.C. 1985, c. N-5, s. 273.65(2)(d).
131 2008 SCC 38, [2008] 2 S.C.R. 326.
132 AIVFA Final Written Submission, p. 92.

4.7.3 Reconciling Secrecy and Disclosure in Allowing Warrants to Be Challenged: The Current Editing Solution

Disclosure of the underlying affidavit is required when the prosecution introduces evidence from an electronic surveillance warrant issued under the *Criminal Code*. The Code allows for the editing of the affidavit before it is disclosed, to protect a broad range of public interests that could be harmed by disclosure. These interests include the identity of a confidential informant, information about ongoing investigations, information that might endanger persons engaged in intelligence-gathering techniques and information that might harm the interests of innocent persons.[133]

The Code permits the disclosure of judicial summaries of the affidavit instead of the whole affidavit. However, the judge is required to order more extensive disclosure of the contents of the affidavit, upon the request of the accused, if the judge believes that a judicial summary would not be sufficient to allow the accused to make full answer and defence.[134] The accused may also be entitled, in certain instances, to cross-examine the person who swore or affirmed the truthfulness of the information in the affidavit.

The process of editing affidavits before disclosure can be time-consuming. Moreover, it produces an artificial basis on which to determine the legality and constitutionality of the warrant because material that is deleted from the affidavit and not disclosed to the accused cannot be used by the Crown to prove the validity of the warrant. The rationale for this is sound. Material that is not disclosed to the accused generally cannot be subject to adversarial challenge.

The editing process can protect important secrets, but it often comes at the high price of making it difficult for the Government to justify the granting of the warrant in the first place. The process of attempting to defend the granting of a warrant without reference to material that is edited out to protect secrets has led to the collapse of at least one terrorism prosecution in Canada. In *R. v. Parmar*,[135] a prosecution against Talwinder Singh Parmar and others failed because the Crown decided not to disclose information in an affidavit that would have revealed the identity of a confidential informer. The informer in that case refused to allow the informer's name to be disclosed and also refused to enter a witness protection program. The Crown was unable to justify the granting of the *Criminal Code* wiretap warrant without referring to material that would have identified the informant. As a result, the court found the warrant to be illegal. At the time, the *Criminal Code* required the exclusion of illegally obtained wiretaps, and the prosecution ended as a result.

---

133 *Criminal Code*, s. 187(4).
134 *Criminal Code*, s. 187(7).
135 (1986) 34 C.C.C.(3d) 260 (Ont. H.C.J.); (1987) 37 C.C.C. (3d) 300 (Ont. H.C.J.); (1987) 31 C.R.R. 256 (Ont. H.C.J.). This case is discussed in Roach Paper on Terrorism Prosecutions.

If a similar case arose today, the wiretap evidence might be admissible at trial. Even if the edited affidavit no longer justified granting the warrant, the Crown might argue that the fruits of the unconstitutional and illegal warrant should be admitted because to do so would not bring the administration of justice into disrepute – the test under section 24(2) of the *Charter* for excluding the wiretap evidence.

The present approach to reconciling the need for disclosure and secrecy involves an editing process pioneered in the *Parmar* case. Although it is fair to the accused, this editing process weakens the Crown's case for the issuance of the warrant. As recommended for the *CSIS Act*, the current *Criminal Code* procedure should be modernized to incorporate better ways to reconcile the competing interests of disclosure and secrecy, while still allowing effective adversarial challenge of the warrant.

4.7.4 The Use of Special Advocates in Proceedings to Challenge *CSIS Act* and *Criminal Code* Warrants

A different approach to disclosure can allow full adversarial challenge to the legality and the constitutionality of the warrant while ensuring that the accused and the public do not gain access to highly sensitive information. This approach involves giving a security-cleared special advocate complete access to the unedited affidavit used to obtain the warrant and to all other relevant information. The special advocate could represent the interests of the accused in challenging the warrant and in seeking the exclusion of evidence obtained under the warrant, without disclosing sensitive information to the accused and the public.

Special advocates are security-cleared lawyers who receive access to secret material that is not seen by the affected person, and who represent the interests of that person. Special advocates cannot disclose or discuss the material with the accused or with anyone else. The *Immigration and Refugee Protection Act*[136] provides a precedent. It was amended to create a statutory regime for special advocates in response to the 2007 Supreme Court decision in *Charkaoui v. Canada*[137] that the complete lack of adversarial challenge to secret evidence used in security certificate cases was an unjustified violation of section 7 of the *Charter*. That statutory regime currently applies only to immigration law proceedings, but the Federal Court has appointed security-cleared *amici curiae* to assist it in a similar manner in proceedings under section 38 of the *Canada Evidence Act*.[138] Two parliamentary committees that conducted reviews of the *Anti-terrorism Act* both recommended that security-cleared counsel be provided

136 S.C. 2001, c. 27. The amendment was introduced by S.C. 2008, c.3. A challenge under ss. 2 and 7 of the Charter to restrictions placed on the ability of special advocates to communicate after having seen secret information was dismissed as premature: *Almrei (Re)*, 2008 FC 1216, 331 F.T.R. 301.

137 *Charkaoui v. Canada (Citizenship and Immigration)*, 2007 SCC 9, [2007] 1 S.C.R. 350.

138 *Khadr v. Canada (Attorney General)*, 2008 FC 46, 54 C.R. (6th) 76; *Canada (Attorney General) v. Khawaja*, 2008 FC 560; *Khadr v. Canada (Attorney General)*, 2008 FC 807.

in legal proceedings to allow adversarial challenge to secret material that the affected person was not allowed to see.[139]

Special advocates could play an important role in testing the validity of warrants issued under section 21 of the *CSIS Act* or under Part VI of the *Criminal Code*. They could be used in terrorism cases involving confidential information that, if disclosed to the accused, could impede ongoing investigations, reveal confidential methods of investigation or the identity of confidential informants or violate promises to third parties not to disclose the identity of confidential informants.

Some groups cautioned against expanding the use of special advocates. Both the Canadian Bar Association and the Federation of Law Societies supported using special advocates in proceedings under section 38 of the *Canada Evidence Act*, but warned against their use in other proceedings and also against other special rules in criminal proceedings. The Criminal Lawyers' Association argued that existing disclosure rules adequately protected the interests of the accused.

The defence may be concerned about introducing a special advocate into criminal trials on the merits because the special advocate participates in only a limited way in the trial. However, in *R. v. Pires; R. v. Lising*, the Supreme Court recognized that proceedings to challenge the legality and constitutionality of a warrant and to seek the exclusion of evidence obtained as a result of a search differ from a criminal trial on the merits of the allegation. Charron J. explained:

> At trial, the guilt or innocence of the accused is at stake. The Crown bears the burden of proving its case beyond a reasonable doubt. In that context, the right to cross-examine witnesses called by the Crown "without significant and unwarranted constraint" becomes an important component of the right to make full answer and defence… If, through cross-examination, the defence can raise a reasonable doubt in respect of any of the essential elements of the offence, the accused is entitled to an acquittal…. However, the…review hearing [to challenge the warrant] is not intended to test the merits of any of the Crown's allegations in respect of the offence. The truth of the allegations asserted in the affidavit as they relate to the essential elements of the offence remain to be proved by the Crown on the trial proper. Rather, the

---

139 House of Commons Canada, Final Report of the Standing Committee on Public Safety and National Security, Subcommittee on the Review of the *Anti-terrorism Act, Rights, Limits, Security: A Comprehensive Review of the Anti-terrorism Act and Related Issues*, March 2007, p. 81, online: Parliament of Canada <http://www2.parl.gc.ca/content/hoc/Committee/391/SECU/Reports/RP2798914/sterrp07/sterrp07-e.pdf> (accessed July 30, 2009); The Senate of Canada, F*undamental Justice In Extraordinary Times: Main Report of the Special Senate Committee on the Anti-terrorism Act*, February 2007, p. 42, online: Parliament of Canada <http://www.parl.gc.ca/39/1/parlbus/commbus/senate/Com-e/anti-e/rep-e/rep02feb07-e.pdf> (accessed July 30, 2009).

> review is simply an evidentiary hearing to determine the *admissibility* of relevant evidence about the offence obtained pursuant to a presumptively valid court order….the statutory preconditions for wiretap authorizations will vary depending on the language of the provision that governs their issuance. The reviewing judge…only inquires into whether there was any basis upon which the authorizing judge could be satisfied that the relevant statutory preconditions existed… Even if it is established that information contained within the affidavit is inaccurate, or that a material fact was not disclosed, this will not necessarily detract from the existence of the statutory pre-conditions….In the end analysis, the admissibility of the wiretap evidence will not be impacted under s. 8 if there remains a sufficient basis for issuance of the authorization.[140]

The special advocate would have access to all the material used to support the application for a warrant, including material that could never be disclosed to the accused. The special advocate would also have access to material disclosed to the accused in accordance with *Stinchcombe*. The accused and the accused's lawyers would provide relevant information about the case to the special advocate. The special advocate could cross-examine a person on the affidavit under the same tests that now allow the accused in certain circumstances to engage in such cross-examination when the truthfulness of the underlying affidavit has been put into question. As well, abuses by state actors that may never come to light due to redactions imposed by Government counsel can be explored by special advocates, possibly affecting the admissibility of the information under section 24(2) of the *Charter*.

Introducing special advocates would affect how trial courts handle confidential information. At present, documents relating to *Criminal Code* electronic surveillance warrants are kept by the trial court at a place to which the public has no access.[141] In investigations of terrorism offences, especially those involving warrants issued under section 21 of the *CSIS Act*, the full affidavit would contain sensitive information relating to national security, national defence or international relations.

Introducing special advocates to challenge wiretaps in terrorism cases could be an important reform. It could make it much easier to use secret intelligence in criminal prosecutions, while retaining the important safeguard, through special advocates, of full adversarial challenge to the warrant. Investigators would no longer have to worry that their legitimate efforts to protect informants, ongoing investigations and information that has been provided with caveats on disclosure, would jeopardize the validity of the warrant. Secret intelligence would no longer be a "poison pill" that would need to be edited out and that could result in the warrant being found to be illegal or unconstitutional.

---

140 *R. v. Pires; R. v. Lising*, 2005 SCC 66, [2005] 3 S.C.R. 343 at paras. 29-30.
141 *Criminal Code*, s. 187(1).

Recommendation 12:

In terrorism prosecutions, special advocates, given powers similar to those permitted under the *Immigration and Refugee Protection Act*, should be allowed to represent the accused in challenging warrants issued under section 21 of the *CSIS Act* or under Part VI of the *Criminal Code*. The special advocates should have access to all relevant information, including unedited affidavits used to justify the warrants, but should be prohibited from disclosing this information to anyone without a court order. Both the judges reviewing the validity of warrants and the special advocates should be provided with facilities to protect information that, if disclosed, might harm national security.

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

CHAPTER V: THE DISCLOSURE AND PRODUCTION OF INTELLIGENCE

5.0 Introduction

Most of the difficulties in managing the relationship between intelligence and evidence involve the need to reconcile broad disclosure requirements with the need for secrecy.

This chapter describes how intelligence can be subject to disclosure and production obligations in terrorism prosecutions. It also examines the possibility of placing limits on disclosure and production obligations, and whether such limits will help to produce a more reliable relationship between intelligence and evidence.

5.1 Disclosure of Information

The accused's right to disclosure is an important constitutional value. As the Supreme Court of Canada explained in *Stinchcombe*:

> [T]here is the overriding concern that failure to disclose impedes the ability of the accused to make full answer and defence. This common law right has acquired new vigour by virtue of its inclusion in s.7 of the *Canadian Charter of Rights and Freedoms* as one of the principles of fundamental justice…. The right to make full answer and defence is one of the pillars of criminal justice on which we heavily depend to ensure that the innocent are not convicted.[1]

The concern for fairness and the intention to prevent miscarriages of justice that animated *Stinchcombe* apply with equal force in terrorism cases. A wrongful terrorism offence conviction stemming from a failure by the Crown to make full disclosure would constitute an injustice. Convicting the innocent would allow the guilty to go free. As well, miscarriages could undermine

---

1 *R. v. Stinchcombe*, [1991] 3 S.C.R. 326 at 336.

public confidence in the justice system, as the Director of Public Prosecutions for England and Wales states:

> Compromising the integrity of the trial process would blight the criminal justice system for decades. It would severely undermine public confidence. We should recall the impact the Birmingham Six case had on public confidence in the 1970s and 1980s. Nothing is more offensive to the Constitution of a country than men and women sitting for years in prison cells for offences they did not commit. What better way could there be to create disillusionment and alienation? We don't want to alienate the very sections of the community whose close cooperation and consent is required to bring successful cases.[2]

Disclosure rights in Canadian law are broad. Former RCMP Commissioner Zaccardelli testified that Canada has "the most liberal disclosure laws in the world."[3] Under *Stinchcombe*, the Crown is required to disclose all relevant information and non-privileged information in its possession to comply with section 7 of the *Charter*, whether the information is inculpatory or exculpatory, and whether or not it is going to be presented as evidence.

In *Stinchcombe*, the Supreme Court saw disclosure as being necessary to respect the rights of the accused to a fair trial and to make full answer and defence. This is consistent with the direction of Justice Rand of the same Court in *Boucher v. The Queen*,[4] where the role of the Crown was described as being to lay before a jury what the Crown considers to be credible evidence relevant to what is alleged to be a crime, and not to obtain a conviction.

Although *dicta* in some cases suggest that material should be disclosed under *Stinchcombe* if it is not clearly irrelevant, the constitutional principle is that the information must be disclosed only if it is relevant to the case. In *Stinchcombe*, Justice Sopinka wrote that it was not necessary to disclose what was "clearly irrelevant."[5] However, he referred to "…the general principle that information ought not to be withheld if there is a reasonable possibility that the withholding of information will impair the right of the accused to make full answer and defence, unless the non-disclosure is justified by the law of privilege."[6]

More recent articulations of disclosure obligations stress the need to disclose all relevant information. For example, in the 2003 decision in *R. v. Taillefer; R v. Duguay*, the Supreme Court described disclosure obligations as follows:

---

2 Ken MacDonald, Q.C., "Security and Rights" (Criminal Bar Association Speech delivered on January 23, 2007), online: Matrix <http://www.matrixlaw.co.uk/showDocument.aspx?documentId=14861> (accessed June 5, 2009).

3 Testimony of Giuliano Zaccardelli, vol. 86, November 30, 2007, p. 11036.

4 [1955] S.C.R. 16 at 23-24.

5 [1991] 3 S.C.R. 326 at 339.

6 [1991] 3 S.C.R. 326 at 340.

> The Crown must disclose all relevant information to the accused, whether inculpatory or exculpatory, subject to the exercise of the Crown's discretion to refuse to disclose information that is privileged or plainly irrelevant. Relevance must be assessed in relation both to the charge itself and to the reasonably possible defences. The relevant information must be disclosed whether or not the Crown intends to introduce it in evidence, before election or plea (p. 343). Moreover, all statements obtained from persons who have provided relevant information to the authorities should be produced notwithstanding that they are not proposed as Crown witnesses (p. 345). This Court has also defined the concept of "relevance" broadly, in *R. v. Egger*, [1993] 2 S.C.R. 451, at p. 467:
>
> One measure of the relevance of information in the Crown's hands is its usefulness to the defence: if it is of some use, it is relevant and should be disclosed — *Stinchcombe*, *supra*, at p. 345. This requires a determination by the reviewing judge that production of the information can reasonably be used by the accused either in meeting the case for the Crown, advancing a defence or otherwise in making a decision which may affect the conduct of the defence such as, for example, whether to call evidence.
>
> As the courts have defined it, the concept of relevance favours the disclosure of evidence. Little information will be exempt from the duty that is imposed on the prosecution to disclose evidence. As this Court said in *Dixon*…"the threshold requirement for disclosure is set quite low.... The Crown's duty to disclose is therefore triggered whenever there is a reasonable possibility of the information being useful to the accused in making full answer and defence"…. "While the Crown must err on the side of inclusion, it need not produce what is clearly irrelevant" (*Stinchcombe, supra*, at p. 339).[7]

In 2009, in *R. v. McNeil*, the Court again described the breadth of *Stinchcombe* disclosure obligations:

> The Crown's obligation to disclose all relevant information in its possession relating to the investigation against an accused is well established. The duty is triggered upon request and does not require an application to the court. *Stinchcombe* made clear that relevant information in the first party production context includes not only information related

7 2003 SCC 70, [2003] 3 S.C.R. 307 at paras. 59-60.

> to those matters the Crown intends to adduce in evidence against the accused, but also any information in respect of which there is a reasonable possibility that it may assist the accused in the exercise of the right to make full answer and defence (pp. 343-44). The Crown's obligation survives the trial and, in the appellate context, the scope of relevant information therefore includes any information in respect of which there is a reasonable possibility that it may assist the appellant in prosecuting an appeal.
>
> While the *Stinchcombe* automatic disclosure obligation is not absolute, it admits of few exceptions. Unless the information is clearly irrelevant, privileged, or its disclosure is otherwise governed by law, the Crown must disclose to the accused all material in its possession. The Crown retains discretion as to the manner and timing of disclosure where the circumstances are such that disclosure in the usual course may result in harm to anyone or prejudice to the public interest. The Crown's exercise of discretion in fulfilling its obligation to disclose is reviewable by a court.[8]

A corollary of the Crown's disclosure obligations under *Stinchcombe* is "…the obligation of the police (or other investigating state authority) to disclose to the Crown all material pertaining to its investigation of the accused."[9] It is not clear whether or when CSIS will be considered to be an "investigating state authority" subject to disclosure duties under *Stinchcombe*. As discussed below, the trial judge in *Malik and Bagri* held that, on the particular facts of the Air India investigation, CSIS was subject to the *Stinchcombe* disclosure requirements. Although the Supreme Court has rejected the notion that "…all state authorities constitute a single indivisible Crown entity for the purposes of disclosure,"[10] it has also indicated that an "investigating state authority" other than the police may be subject to disclosure obligations under *Stinchcombe*. The Court called for the Crown to make reasonable inquiries to facilitate disclosure and to "…bridge much of the gap between first party disclosure and third party production" when the prosecutor knows that another Crown agency has been involved with the investigation.[11] For instance, the prosecutor will usually be aware of CSIS involvement in a terrorism investigation.

---

8 2009 SCC 3 at paras. 17-18.

9 *R. v. McNeil*, 2009 SCC 3 at para. 14.

10 *R. v. McNeil*, 2009 SCC 3 at para. 13.

11 *R. v. McNeil*, 2009 SCC 3 at para. 51. See also para. 49, quoting with approval *R. v. Arsenault* (1994), 153 N.B.R. (2d) 81 at para. 15 (C.A.): "When disclosure is demanded or requested, Crown counsel have a duty to make reasonable inquiries of other Crown agencies or departments that could reasonably be considered to be in possession of evidence. Counsel cannot be excused for any failure to make reasonable inquiries when to the knowledge of the prosecutor or the police there has been another Crown agency involved in the investigation. Relevancy cannot be left to be determined by the uninitiated. If Crown counsel is denied access to another agency's file, then this should be disclosed to the defence so that the defence may pursue whatever course is deemed to be in the best interests of the accused. This also applies to cases where the accused or defendant, as the case may be, is unrepresented…"

The right to disclosure under *Stinchcombe* is not absolute. The Supreme Court was cognizant of the danger that disclosure of information might "…put at risk the security and safety of persons who have provided the prosecution with information."[12] It held that the Crown would not have to disclose information that was covered by police informer privilege or by any other privilege. Thus, the Crown would not have to disclose the identities of informers who were promised anonymity by the police in exchange for information. The Crown would also have a reviewable discretion to withhold the identities of persons "… to protect them from harassment or injury, or to enforce the privilege relating to informers," and would have a reviewable discretion to delay disclosure "… in order to complete an investigation."[13] In addition, as discussed in depth in Chapter VII, the Crown could seek specific non-disclosure orders under sections 37 and 38 of the *Canada Evidence Act*.[14] The Court described the exceptions to the obligation to disclose as follows:

> [T]his obligation to disclose is not absolute. It is subject to the discretion of counsel for the Crown. This discretion extends both to the withholding of information and to the timing of disclosure. For example, counsel for the Crown has a duty to respect the rules of privilege. In the case of informers the Crown has a duty to protect their identity. In some cases serious prejudice or even harm may result to a person who has supplied evidence or information to the investigation. While it is a harsh reality of justice that ultimately any person with relevant evidence must appear to testify, the discretion extends to the timing and manner of disclosure in such circumstances. A discretion must also be exercised with respect to the relevance of information. While the Crown must err on the side of inclusion, it need not produce what is clearly irrelevant…. The initial obligation to separate "the wheat from the chaff" must therefore rest with Crown counsel. There may also be situations in which early disclosure may impede completion of an investigation. Delayed disclosure on this account is not to be encouraged and should be rare. Completion of the investigation before proceeding with the prosecution of a charge or charges is very much within the control of the Crown. Nevertheless, it is not always possible to predict events which may require an investigation to be re-opened and the Crown must have some discretion to delay disclosure in these circumstances.[15]

---

12 [1991] 3 S.C.R. 326 at 335.
13 [1991] 3 S.C.R. 326 at 336.
14 R.S.C. 1985, c. C-5.
15 *R. v. Stinchcombe*, [1991] 3 S.C.R. 326 at 339-340.

5.2 Retention of Information

The right to disclosure has been interpreted by the Supreme Court to include a duty under section 7 of the *Charter* to retain relevant information that is subject to disclosure obligations.[16] In *Malik and Bagri*, Justice Josephson found a breach of section 7, as there was an unacceptable degree of negligence in the destruction by CSIS of the Parmar wiretaps and the notes of the interviews with Ms. E.

As the Hon. Bob Rae stated in his report:

> The erasure of the tapes is particularly problematic in light of the landmark decision of the Supreme Court of Canada in *R. v. Stinchcombe*, which held that the Crown has a responsibility to disclose all relevant evidence to the defence even if it has no plans to rely on such evidence at trial. Justice Josephson held that all remaining information in the possession of CSIS is subject to disclosure by the Crown in accordance with the standards set out in *Stinchcombe*. Accordingly, CSIS information should not have been withheld from the accused.[17]

The Supreme Court reasoned, in its 1997 decision in *R. v. La,* that "… [t]he right of disclosure would be a hollow one if the Crown were not required to preserve evidence that is known to be relevant."[18] As discussed in Chapter IV, the Court recently reminded CSIS of the importance of retaining the intelligence that it collects about specific individuals and groups, in part because the intelligence may later be subject to disclosure obligations.[19] However, the duty to retain information that might subsequently have to be disclosed is not absolute. It would be unrealistic and impractical to expect every piece of material to be retained "…on the off-chance that it will be relevant in the future."[20]

The duty to retain relevant material for disclosure can benefit both the accused and the state. It is still not possible to determine whether the material that was destroyed in the Air India investigation would have assisted the accused or the prosecution, or whether it would have been of little value to either. This disturbing uncertainty underscores the importance of CSIS retaining intelligence that could become relevant in a terrorism prosecution, a topic already discussed at length in Chapter IV.

---

16 *R. v. La*, [1997] 2 S.C.R. 680.
17 *Lessons to be Learned: The report of the Honourable Bob Rae, Independent Advisor to the Minister of Public Safety and Emergency Preparedness, on outstanding questions with respect to the bombing of Air India Flight 182* (Ottawa: Air India Review Secretariat, 2005), p. 16.
18 [1997] 2 S.C.R. 680 at para. 20.
19 *Charkaoui v. Canada*, 2008 SCC 38, [2008] 2 S.C.R. 326.
20 *R. v. La*, [1997] 2 S.C.R. 680 at para. 21.

5.3 The "Relevance" Requirement

In its 1993 decision in *R. v. Egger*, the Court re-iterated that "… [o]ne measure of the relevance of information in the Crown's hands is its usefulness to the defence: if it is of some use, it is relevant and should be disclosed…. This requires a determination by the reviewing judge that production of the information can reasonably be used by the accused either in meeting the case for the Crown, advancing a defence or otherwise in making a decision which may affect the conduct of the defence such as, for example, whether to call evidence."[21]

In 1995, the Court held in *R. v. Chaplin*[22] that the Crown did not need to disclose wiretaps that did not relate to the particular charges faced by the accused:

> Fishing expeditions and conjecture must be separated from legitimate requests for disclosure. Routine disclosure of the existence of wiretaps in relation to a particular accused who has been charged, but who is the subject of wiretaps for ongoing criminal investigations in relation to other suspected offences, would impede the ability of the state to investigate a broad array of sophisticated crimes which are otherwise difficult to detect, such as drug-trafficking, extortion, fraud and insider trading: *R. v. Duarte*, [1990] 1 S.C.R. 30, at p. 44. Wiretaps are generally only effective if their existence is unknown to the persons under investigation.[23]

Chaplin could be germane to discussions about disclosing intelligence. The case contemplated that some investigative materials that do not relate to the charges faced by the accused may not be subject to disclosure. It also affirmed that the Crown does not have to disclose material that is beyond its control. In addition, once the Crown affirms that it has satisfied its disclosure obligations, the defence must "…establish a basis which could enable the presiding judge to conclude that there is in existence further material which is potentially relevant."[24]

In a recent report on large and complex criminal case procedures, the Hon. Patrick Lesage and Professor (now Justice) Michael Code relied on *Chaplin* for the proposition that the defence can obtain disclosure of material that lies outside the core disclosure obligations, but the defence must first justify such

---

21 [1993] 2 S.C.R. 451 at 467.

22 [1995] 1 S.C.R. 727. For further discussion of this case and its relevance to the disclosure of intelligence, see Kent Roach, "The Unique Challenges of Terrorism Prosecutions: Towards a Workable Relation Between Intelligence and Evidence" in Vol. 4 of Research Studies: The Unique Challenges of Terrorism Prosecutions, pp. 129-131 [Roach Paper on Terrorism Prosecutions].

23 [1995] 1 S.C.R. 727 at para. 32.

24 [1995] 1 S.C.R. 727 at para. 30.

disclosure.[25] Material that the defence demonstrates is not clearly irrelevant, or that is of potential relevance, can be made available to the defence for inspection at a secure location, if need be. This can avoid the need for the Crown to copy and produce, literally, truckloads of documents.

The Supreme Court has also repeatedly stated that not every violation of the accused's right to disclosure will impair the right to make full answer and defence or make a fair trial impossible.[26] A trial may be fair even if the accused does not receive all relevant material. The courts have also accepted that reasonable explanations about why relevant material has been destroyed and is not available for disclosure may lead to a finding that there was no violation of the right to disclosure.[27]

5.4 Applying *Stinchcombe* to Intelligence

Some concerns were expressed during the Commission hearings that the *Stinchcombe* disclosure requirements would be unworkably broad if applied to intelligence.[28] The extent of the disclosure obligations imposed by *Stinchcombe* should not be exaggerated. The basic rule that the state does not have to disclose irrelevant or privileged material can shield much intelligence from disclosure and prevent fishing expeditions by defence counsel. In several recent cases, courts have found that *Stinchcombe* disclosure obligations do not apply to material such as analytical intelligence, documents that were internal to the working of security intelligence agencies or that involved communications with foreign agencies, and intelligence relating to suspects and investigations that were unrelated to the accused. This was because these materials were not relevant to the charges faced by the accused and were of no possible use to the accused.[29]

The important role of prosecutors in managing the disclosure process is discussed in Chapter IX. That chapter also discusses the equally important role of the trial judge in supervising the disclosure process and in preventing frivolous motions for disclosure.

---

25 Patrick Lesage and Michael Code, Report of the Review of Large and Complex Criminal Case Procedures (November 2008), pp. 45-55, online: Ontario Ministry of the Attorney General <http://www.attorneygeneral.jus.gov.on.ca/english/about/pubs/lesage_code/lesage_code_report_en.pdf> (accessed December 5, 2008) [Lesage and Code Report on Large and Complex Criminal Case Procedures].

26 R. v. Dixon, [1998] 1 S.C.R. 244; R. v. Taillefer; R. v. Duguay, 2003 SCC 70, [2003] 3 S.C.R. 307.

27 R. v. Stinchcombe, [1995] 1 S.C.R. 754; R. v. La, [1997] 2 S.C.R. 680.

28 See generally the testimony given by members of the panel discussing the interaction between Stinchcombe and s. 38 of the Canada Evidence Act, vol. 86, November 30, 2007, pp. 11105-11124.

29 Nicholas Ribic and Her Majesty the Queen and Canadian Security Intelligence Service, 2002 FCT 290 at paras. 7-10; Canada (Attorney General) v. Ribic, 2003 FCA 246, 185 C.C.C. (3d) 129 at paras. 40-41; Canada (Attorney General) v. Khawaja, 2007 FC 490, 219 C.C.C. (3d) 305 at para. 116, reversed in part on other grounds 2007 FCA 342; Canada (Attorney General) v. Khawaja, 2008 FC 560 at para. 14; Khadr v. Canada (Attorney General), 2008 FC 807, 331 F.T.R. 1 at para. 68.

5.4.1 The Role of *Stinchcombe* in the Air India Prosecutions

Stinchcombe disclosure obligations presented serious challenges in the Malik and Bagri prosecution, both in relation to the logistics of disclosure and, more particularly, in relation to the retention and disclosure of CSIS intelligence.

CSIS was held to be subject to *Stinchcombe* disclosure requirements on the particular facts of the Air India investigation. In 2002, Justice Josephson observed that, "Mr. Code for Mr. Bagri persuasively submits that both law and logic lead to a conclusion that, in the circumstances of this case, C.S.I.S. is part of the Crown" [30] and, as a result, was subject to *Stinchcombe* disclosure obligations. The Crown conceded that *Stinchcombe* applied to CSIS as a result of a 1987 agreement that the RCMP would have "…unfettered access to all relevant information in the files of C.S.I.S." about the investigation.[31] This led Justice Josephson to conclude that "…all remaining information in the possession of C.S.I.S. is subject to disclosure by the Crown in accordance with the standards set out in *R. v. Stinchcombe*."[32] However, the acquittal of the accused made his conclusion academic.

In 2004, the Crown again conceded that *Stinchcombe* applied to CSIS as a result of the 1987 agreement between CSIS and the RCMP. Justice Josephson concluded that, even without the agreement, evidence obtained by CSIS that was relevant to the Air India investigation should have been passed on to the RCMP:

> Despite clear lines of demarcation between the roles of C.S.I.S. and the R.C.M.P., the information obtained from the Witness immediately struck [the CSIS agent] as being of extreme importance and relevance to the Air India criminal investigation. When, in the course of his information gathering role, he uncovered evidence relevant to that investigation, he was obliged by statute and policy to preserve and pass on that evidence to the R.C.M.P.[33]

The duty of CSIS to retain such intelligence was affirmed by the Supreme Court of Canada in its 2008 decision in *Charkaoui*.[34] Under an amended section 19 of the *CSIS Act*,[35] as recommended in Chapter IV, CSIS would be obliged to share relevant information with either the RCMP or the National Security Advisor (NSA). In this way, the amount of CSIS information that would be subject to disclosure would increase.

5.4.2 The Effect of *Stinchcombe* on CSIS/RCMP Cooperation

The Commission heard much testimony about *Stinchcombe*. RCMP Deputy Commissioner Gary Bass described *Stinchcombe* as having resulted in "…the

---

30 *R. v. Malik, Bagri and Reyat*, 2002 BCSC 864 at para. 9.
31 2002 BCSC 864 at para. 10.
32 2002 BCSC 864 at para. 14.
33 *R. v. Malik and Bagri*, 2004 BCSC 554, 119 C.R.R. (2d) 39 at para. 20.
34 *Charkaoui v. Canada* (Citizenship and Immigration), 2008 SCC 38, [2008] 2 S.C.R. 326.
35 *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23.

single most draining set of processes to policing…in the history of policing."[36] The interpretation of *Stinchcombe* by Jack Hooper, a former Deputy Director of CSIS, differed from Bass's "fairly absolute interpretation." Hooper testified that the idea of full disclosure was a "worst-case scenario" that discounted the possibility that intelligence would either be found not to be relevant to the specific criminal charges or that it would be protected by national security privilege.[37]

Jim Judd, the Director of CSIS, testified that "…it would be useful to have some mechanism whereby the information in our holdings that was not relevant to the criminal prosecution…[was] protected and excluded because we have sources who report on multiple issues, multiple situations."[38]

The requirement of relevance under *Stinchcombe* can protect some intelligence from disclosure. Analyses about general security threats, intelligence or information about third parties who play no role in a prosecution, information about third parties who are not related to the accused,[39] and internal administrative matters within a police force or a security intelligence agency will generally not be relevant or helpful to the accused. As a result, they will not have to be disclosed to comply with *Stinchcombe*.

Nevertheless, some view *Stinchcombe* as a major impediment to cooperation between CSIS and the RCMP. In a 1998 report, the Security Intelligence Review Committee warned that, because of *Stinchcombe*, "…all CSIS intelligence disclosures, regardless of whether they would be entered for evidentiary purposes by the Crown, are subject to disclosure to the Courts. Any passing of information, whether an oral disclosure or in a formal advisory letter, could expose CSIS investigations. This means that even information that is provided during joint discussions on investigations or that is provided as an investigative lead is at risk."[40] It concluded that the disclosure problem represented by *Stinchcombe* seemed to be "insoluble" and that it "…carried the potential to disrupt CSIS-RCMP relationships and could potentially damage the operation of both agencies."[41] In their papers for the Commission, Professors Wark and Brodeur both commented that *Stinchcombe* has been interpreted as an impediment to RCMP/CSIS cooperation, particularly because of CSIS concerns about the disclosure of secret human sources and the possible use of intelligence as evidence.[42]

---

36 Testimony of Gary Bass, vol. 87, December 3, 2007, p. 11279.
37 Testimony of Jack Hooper, vol. 50, September 21, 2007, pp. 6216-6217.
38 Testimony of Jim Judd, vol. 90, December 6, 2007, p. 11887.
39 *Khadr v. Canada* (Attorney General), 2008 FC 807, 331 F.T.R. 1 at para. 68.
40 Security Intelligence Review Committee, *CSIS Co-Operation with the RCMP - Part I* (SIRC Study 1998-04), October 16, 1998, p. 9 [SIRC Study 1998-04].
41 SIRC Study 1998-04, p. 18.
42 Wesley Wark, "The Intelligence-Law Enforcement Nexus: A study of co-operation between the Canadian Security Intelligence Service and the Royal Canadian Mounted Police, 1984-2006, in the Context of the Air India terrorist attack" in Vol. 1 of Research Studies: Threat Assessment RCMP/CSIS Co-operation, pp. 164-165; Jean-Paul Brodeur, "The Royal Canadian Mounted Police and the Canadian Security Intelligence Service: A Comparison Between Occupational and Organizational Cultures" in Vol. 1 of Research Studies: Threat Assessment RCMP/CSIS Co-operation, p. 204.

The extent to which, and when, CSIS is subject to *Stinchcombe* disclosure obligations continues to evolve. Courts of appeal are divided about when agencies other than the police are subject to *Stinchcombe* disclosure obligations. The New Brunswick Court of Appeal held that the Crown should include material held by another Crown agency involved in the investigation,[43] while the Alberta Court of Appeal held that provincial Crowns should not be required to disclose material held by federal agencies beyond their control.[44] The Supreme Court of Canada's 2009 decision in *McNeil* [45] did not resolve the issue for CSIS. The Court clearly dismissed as unworkable the idea that all state agencies are subject to *Stinchcombe*. The Court noted, however, that investigating authorities other than the police may be subject to *Stinchcombe* disclosure requirements and that, in any event, the Crown has an obligation to inquire about whether other investigating agencies have material that is likely relevant to the proceedings. Increased integration of the RCMP and CSIS may point to more frequent court findings that CSIS is subject to *Stinchcombe*.

5.5 Potential Changes to the Approach to Disclosure

Some intervenors, including the Canadian Bar Association and the Criminal Lawyers' Association, argued that the Air India case did not reveal a demonstrable need for change in the approach to disclosure and that it therefore could not provide a sound basis for making general recommendations in this area.[46]

In his Final Submissions, the Attorney General of Canada acknowledged the challenges presented by the requirement to disclose large amounts of material, but cautioned against a recommendation that legislation be enacted to clarify *Stinchcombe*. He warned about unforeseen consequences and about the complexity of legislating federally on a matter that affected provincial jurisdiction.[47]

No party or intervenor before the Commission proposed adopting legislation to attempt to abolish or limit *Stinchcombe* disclosure obligations. Some intervenors, including the Canadian Association of Chiefs of Police and the Air India Victims Families Association, called for clarification of, and guidelines about, the extent and particular obligations of *Stinchcombe*.[48] The Air India Victims Families Association asked that the guidelines be in the form of legislation. The Canadian

---

43 *R. v. Arsenault* (1994), 93 C.C.C. (3d) 111 (N.B.C.A.).

44 *R. v. Gingras* (1992), 71 C.C.C. (3d) 53 (Alta. C.A.).

45 2009 SCC 3.

46 Canadian Bar Association, Submission to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, April 2007; Submissions of the Criminal Lawyers' Association, February 2008.

47 Final Submissions of the Attorney General of Canada, February 29, 2008, Vol. III, paras. 80-84 [Final Submissions of the Attorney General of Canada].

48 Canadian Association of Chiefs of Police Written Submissions, pp. 8-9; *Where is Justice?* AIVFA Final Written Submission, Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, February 29, 2008, p. 131.

Association of Chiefs of Police called for a clarification of the roles and obligations of the Crown and police in relation to disclosure and for a move towards electronic disclosure.[49]

The reluctance of the parties and intervenors to ask for limitations on *Stinchcombe* is no doubt related to the status of *Stinchcombe* as a statement of the disclosure required by section 7 of the *Charter*. As the Attorney General of Canada submitted:

> It is a fundamental element of the fair and proper operation of the Canadian criminal justice system that an accused person has the right to the disclosure of all relevant information in the possession or control of the Crown, with the exception of privileged information….The right to proper disclosure is recognized in particular under principles of fundamental justice as necessary to the accused person's ability to defend himself or herself against the charges that have been laid.[50]

A variety of legislative measures to limit the scope of *Stinchcombe* could be enacted to protect intelligence from disclosure. However, the Commission does not recommend any of these measures for the reasons that follow.

One possible measure could be to deem CSIS to be a third party that is not subject to *Stinchcombe* disclosure obligations. Legislation could establish a procedure for requests for production from CSIS. The legislation would include a list of dangers flowing from disclosing secret intelligence that judges should consider before ordering that CSIS material be produced. Such provisions, by preventing judges from determining on the facts of the case whether CSIS material is subject to *Stinchcombe* or not, would inevitably be challenged under the *Charter* as violating the right of the accused to disclosure and the right to make full answer and defence. An accused could cite in his or her support the determination by Justice Josephson in the Malik and Bagri case that CSIS was subject to *Stinchcombe*. In addition, the Supreme Court of Canada held in 2008, in both the *Charkaoui*[51] and *Khadr*[52] cases, that section 7 of the *Charter* may require retention and disclosure of CSIS intelligence even for cases that are not prosecuted in Canada's criminal justice system. In short, deeming CSIS to be a third party (rather than part of the Crown) might not prevent CSIS from being obliged by section 7 to disclose at least some material.

Legislation could also limit *Stinchcombe* by reducing the Crown's disclosure obligations. Legislation could specify that only exculpatory information or information that would undermine the Crown's case be disclosed. However, the Supreme Court has already clearly rejected such a position in *Stinchcombe*

---

49 Canadian Association of Chiefs of Police Written Submissions, p. 9.
50 Final Submissions of the Attorney General of Canada, Vol. III, paras. 31-32.
51 *Charkaoui v. Canada* (Citizenship and Immigration), 2008 SCC 38, [2008] 2 S.C.R. 326.
52 *Canada (Justice) v. Khadr*, 2008 SCC 28, [2008] 2 S.C.R. 125.

and in subsequent judgments dealing with disclosure. Although the Court has not ruled out the possibility that a limit on a section 7 right could be justified as reasonable under section 1 of the *Charter*, it has repeatedly emphasized that the standards for any such limit would be extremely high.[53] Still, the Court has not completely discounted limitations.[54]

Protecting intelligence from disclosure is a sufficiently important goal to justify some limits on section 7 rights.[55] To justify the limits, the Crown should be obliged to demonstrate that there are no less drastic means to protect the intelligence. The Crown's ability to obtain judicial non-disclosure orders under sections 37 and 38 of the *Canada Evidence Act* could be cited as less drastic means. Even if a court concluded that other, less drastic, alternatives were not available, the court would still have to assess the overall balance between the need to protect intelligence from disclosure and the harm to the accused's rights that non-disclosure would cause.

Even under a statutory regime that purported to exempt CSIS from *Stinchcombe* disclosure requirements or to limit disclosure requirements to exculpatory material, the courts would still require CSIS to disclose information to the accused that was necessary for the accused to make full answer and defence and to have a fair trial.

Furthermore, even if legislation limiting *Stinchcombe* could be upheld under the *Charter*, limiting disclosure in advance through legislation would be awkward. It would be difficult for Parliament to predict, without knowing the facts of a particular case, what must and must not be disclosed. General guidelines would be of little use. The legislation might not prevent disclosure of material that is actually not needed to assist the accused but that could, by being disclosed, be very damaging to national security or to CSIS operations. A more practical and efficient means to address the constitutional obligations to disclose intelligence would be to improve the process that can be used to obtain non-disclosure orders on the facts of the particular case. Chapter VII discusses how to improve that process.

RCMP Commissioner William Elliott testified that he was unsure about how practical it would be to create a different procedural regime for terrorism cases, and about how such a regime would work without limiting the ability of the accused to make full answer and defence.[56] Even when protecting vital interests, such as solicitor and client confidences or the identities of informers, the courts have recognized that there must be disclosure when the accused's innocence

---

53 *Re B.C. Motor Vehicle Act*, [1985] 2 S.C.R. 486; *Suresh v. Canada (Minister of Citizenship and Immigration)*, 2002 SCC 1, [2002] 1 S.C.R. 3; *Charkaoui v. Canada (Citizenship and Immigration)*, 2007 SCC 9, [2007] 1 S.C.R. 350; *R. v. D.B.*, 2008 SCC 25, [2008] 2 S.C.R. 3.

54 The Court has recognized that *Stinchcombe* obligations can in some cases, without violating the *Charter*, be limited by statutes in relation to private records in the Crown's possession: R. v. McNeil, 2009 SCC 3 at para. 21, citing *R. v. Mills*, [1999] 3 S.C.R. 668 at para. 59.

55 *Charkaoui v. Canada (Citizenship and Immigration)*, 2007 SCC 9, [2007] 1 S.C.R. 350 at paras. 66-68.

56 Testimony of William Elliott, vol. 90, December 6, 2007, pp. 11809-11810.

is at stake.[57] In short, even aggressive legislative limits on *Stinchcombe* would not provide a reliable guarantee that CSIS material would never be disclosed to the accused. For many reasons, a legislative "quick fix" is not realistic and is not recommended.

5.6 The Need for Guidelines on the Proper Extent of Disclosure

Prosecutors must not overestimate the extent of *Stinchcombe* disclosure obligations in terrorism prosecutions. The practice that sometimes occurs – of producing all information except that which is clearly irrelevant – is of limited value to the accused and should not be the standard practice, although *obiter dicta* from the Supreme Court of Canada suggest otherwise.[58] There is a danger that the reasoning in *dicta* about disclosing material that is not clearly irrelevant has become the operational standard used by prosecutors for disclosure.

A standard of disclosing all material that is not clearly irrelevant could, if applied mechanically, result in disclosure of much material that is of no possible use to the accused. The correct principle, in the Commission's view, is that the Crown need disclose only relevant information to the accused. Information other than this, which is not clearly irrelevant, should be made available to the defence for inspection in a secure environment.[59]

Anne-Marie Boisvert of the University of Montreal expressed the view that:

> I think that Crown prosecutors are sometimes not forceful enough in their objections to some disclosures and the judiciary has sometimes also not been forceful enough, or could have imposed a number of conditions on the disclosure.
>
> Sometimes, I feel that we don't think enough about the consequences, but everyone has powers that they -- and while we are always trying to propose legislative solutions after the fact, I think that we could be more careful. The defendant is entitled to a fair trial, to a full and complete defence. He is not necessarily entitled to publish whatever he wants on the Internet.[60] [Translation]

Similarly, Bruce MacFarlane, a former Deputy Attorney General of Manitoba, agreed that *Stinchcombe* was never intended to require absolute, or all-encompassing, disclosure and observed that prosecutors "…are clearly erring on the side of disclosure." The result was an "absolutely daunting" amount of

---

57 *R. v. McClure*, 2001 SCC 14, [2001] 1 S.C.R. 445; *Named Person v. Vancouver Sun*, 2007 SCC 43, [2007] 3 S.C.R. 252.
58 *R. v. Chaplin*, 1995 CanLII 126, [1995] 1 S.C.R. 727.
59 The procedure for inspection is discussed in Chapter IX.
60 Testimony of Anne-Marie Boisvert, vol. 69, October 30, 2007, p. 8773.

disclosure.[61] This is arguably because it is easier to disclose everything than to select the materials that are relevant.

In the absence of judicial guidance, prosecutors should not be criticized for erring in the direction of more extensive disclosure to ensure fairness to the accused or for interpreting their disclosure obligations broadly. However, prosecutors should use their professional judgment in determining which material must be disclosed. The standard for disclosure should be the relevance standard as it has been articulated consistently by the Supreme Court of Canada in several cases. The Crown also has discretion about when to disclose material. Departures from the usual rule of early pre-trial disclosure may be justified if there are concerns about the safety of informers and witnesses or if there is a need to protect ongoing investigations from being exposed. Delays in disclosure could also be justified when attempts are being made to secure consent to disclosure from third parties, such as foreign intelligence agencies.[62]

The Federal Prosecution Service Deskbook usefully identifies categories of material that should and should not be disclosed. However, the Deskbook should be updated, especially about material that may be the subject of a national security confidentiality claim under section 38 of the *Canada Evidence Act*. The section on national security confidentiality in the current Deskbook has not been revised since 2000.[63] Since 2000, courts have found that time-consuming and disruptive section 38 claims have been made with respect to information that is not relevant to the case and that would not assist the accused.[64]

What must be disclosed can most appropriately and most efficiently be decided by the trial judge. Hence, the early appointment of a trial judge is important in terrorism prosecutions. A staged approach to disclosure, such as that used in the Malik and Bagri prosecution, is also useful, even if it results in some material of only minimal relevance being made available for inspection by the accused. Staged disclosure and the importance of electronic disclosure are discussed in greater depth in Chapter IX.

Recommendation 13:

Federal prosecutorial guidelines should be amended to make it clear to those who prosecute terrorism cases that only material that is relevant to the case and of possible assistance to the accused should be disclosed. Material of limited

---

61 Testimony of Bruce MacFarlane, vol. 78, November 19, 2007, pp. 9931-9932.

62 See Chapter IX for further discussion of the need for staged disclosure in terrorism prosecutions.

63 As suggested by the Table of Contents for the Federal Prosecution Service Deskbook, online: Department of Justice Canada <http://canada.justice.gc.ca/eng/dept-min/pub/fps-sfp/fpd/toc.html> (accessed July 30, 2009).

64 *Nicholas Ribic and Her Majesty the Queen and Canadian Security Intelligence Service*, 2002 FCT 290 at paras. 7-10; *Canada (Attorney General) v. Ribic*, 2003 FCA 246, 185 C.C.C. (3d) 129 at paras. 40-41; *Canada (Attorney General) v. Khawaja*, 2007 FC 490, 291 C.C.C. (3d) 305 at para. 116, reversed on other grounds 2007 FCA 342; *Canada (Attorney General) v. Khawaja*, 2008 FC 560 at para. 14; *Khadr v. Canada (Attorney General)*, 2008 FC 807, 331 F.T.R. 1 at para. 68.

relevance – in the sense that it is not clearly irrelevant – should, in appropriate cases, be made available for inspection by the defence at a secure location.

5.7 Production of Intelligence under *R. v. O'Connor*

Apart from the obligation to disclose pursuant to *Stinchcombe*, CSIS may be the subject of an application to obtain information from a third party. The Supreme Court of Canada's 1995 decision in *R. v. O'Connor* recognizes that the accused can obtain information from third parties, including public and private agencies, where the information relates to an issue at trial, the reliability of evidence or the credibility of witnesses.[65] Still, the authority to obtain access to material from third parties is not absolute. The accused must show that the material held by the third party meets a higher standard of relevance than if that same material were held by the Crown.

The standard with respect to third party information is whether the information is "likely relevant," as opposed to the *Stinchcombe* standard of "relevant."[66] This "likely relevant" threshold is "a significant burden" on the accused, and is designed to stop fishing expectations, but "it should not be interpreted as an onerous burden," given the practical difficulty faced by the accused in trying to establish the relevance of material that he or she has not seen.[67] If the standard is met, a judicial weighing follows of the harms and benefits of producing the document to the accused.

In *McNeil*, the Supreme Court indicated that, if third party records have "true relevance" to the trial, they should generally be disclosed to the accused as they would be disclosed under *Stinchcombe,* although perhaps subject to some editing and restrictions on the use of the material to protect competing interests, such as residual privacy interests.[68] Claims of privilege, such as informer privilege[69] or national security privilege,[70] can be made and can "…bar the accused's application for production of the targeted documents, regardless of their relevance. Issues of privilege are therefore best resolved at the outset of the *O'Connor* process."[71]

Even though *O'Connor* establishes a higher threshold of relevance and limited balancing of the competing interests for and against disclosure of third party records, it could still result in information collected by CSIS in counterterrorism investigations being subject to production. CSIS surveillance material may be highly relevant to many issues in terrorism trials, such as the whereabouts of the accused or associates of the accused, or the credibility of a key witness who had previously provided information to CSIS.

---

65 [1995] 4 S.C.R. 411 at para. 22.
66 *R. v. Mills*, [1999] 3 S.C.R. 668 at paras. 45-47; *R. v. McNeil*, 2009 SCC 3 at para. 33.
67 *R. v. McNeil*, 2009 SCC 3 at para. 29.
68 *R. v. McNeil*, 2009 SCC 3 at paras. 42-47.
69 See Chapter VI for discussion of this and other privileges.
70 See Chapter VII for a discussion of national security privilege under s. 38 of the *Canada Evidence Act*.
71 *R. v. McNeil*, 2009 SCC 3 at para. 27(4).

5.7.1 Legislating Requests for Production of Intelligence under *O'Connor*

There is some precedent for legislation that clarifies the *O'Connor* common law procedures for obtaining production of material from third parties as part of the criminal trial. In *R. v. Mills*,[72] the Supreme Court of Canada upheld legislation enacted in response to *O'Connor*. The legislation provided a procedure and a list of relevant factors for judges to consider before they ordered private information held by third parties or by the Crown about complainants in sexual cases to be produced to the trial judge or disclosed to the accused. The Court's decision was based on the notion that Parliament was reconciling the competing *Charter* rights of the complainant and the accused. Professor Roach, in his study for the Commission, suggested that courts should not apply the same approach if they conclude that the national security context "…pits an individual accused against the admittedly weighty interests of the state."[73]

A restrictive legislative regime governing requests for production from CSIS would not give CSIS any certainty that its intelligence would never be subject to a production or disclosure order. Any legislation would have to allow sufficient judicial discretion to ensure that the accused's right to make full answer and defence was not violated.[74]

There is little reason to conclude that the absence of legislation dealing with third party disclosure will lead judges to become insensitive to the harms that might be caused by producing and disclosing intelligence. Furthermore, legislation that attempted to deem CSIS to be a third party and that restricted the production and disclosure of intelligence could produce much unnecessary litigation. Such legislation would be challenged on the basis that the CSIS material was subject to *Stinchcombe*, as it was held to be in the Malik and Bagri prosecution. Related litigation issues could include whether CSIS was an "investigating state authority" subject to *Stinchcombe* or whether Crown counsel properly exercised their responsibilities as officers of the court to effectively "…bridge much of the gap between first party disclosure and third party production."[75] Litigation about the status of CSIS or the terms or constitutionality of restrictive legislation would lengthen terrorism prosecutions without necessarily resolving the ultimate issue of whether, and in what form, the accused should have access to CSIS material. Roach warned that "…[e]ven if legislation restricting disclosure or production… was upheld under the Charter, there could be much litigation about the precise meaning of the legislation and its relation to Charter standards….The apparent certainty produced by new legislation in protecting intelligence from disclosure may be more illusory than real."[76]

---

72 [1999] 3 S.C.R. 668.
73 Roach Paper on Terrorism Prosecutions, p. 152.
74 *R. v. Taillefer; R. v. Duguay*, 2003 SCC 70, [2003] 3 S.C.R. 307.
75 *R. v. McNeil*, 2009 SCC 3 at paras. 14, 51.
76 Roach Paper on Terrorism Prosecutions, p. 171.

5.8 Anticipating Disclosure

If CSIS information is not already included in the *Stinchcombe* material disclosed to an accused in a terrorism prosecution, the accused will almost inevitably seek production of information that CSIS may hold. This will require time-consuming litigation that may involve judges examining CSIS information in detail. In some cases, it may be appropriate for the Crown voluntarily to include relevant CSIS information as part of the *Stinchcombe* disclosure process, whether or not a court would hold CSIS to be subject to *Stinchcombe* in the particular case. This approach would also ensure that the Crown discharges its duties, articulated in the recent *McNeil* case, to make inquiries about relevant material that should be disclosed in cases where it knows that a CSIS investigation has taken place.[77] It may be more feasible for the Crown to include CSIS information that is not excluded by privilege as part of its *Stinchcombe* disclosure obligations if, as in the Air India trial, the CSIS information is made available for inspection by the defence at a secure location.

In some cases it may be appropriate for the Attorney General of Canada to move directly to obtain a non-disclosure order under section 38 of the *Canada Evidence Act* for information held by CSIS. A preliminary assertion of privilege could preclude the need to decide whether *Stinchcombe* or *O'Connor* procedures apply. Litigation under section 38 would determine whether, and in what form, CSIS material would be disclosed to the accused. Section 38 contemplates measures such as partial redaction or the use of summaries in order to reconcile the competing interests in disclosure and secrecy.

Litigating the disclosure of intelligence under section 38 will address the core issue: whether, and in what form, CSIS intelligence must be disclosed to the accused. It could avoid litigating the somewhat academic issues of whether CSIS is part of the Crown subject to *Stinchcombe* or only a third party in the prosecution, or whether the Crown has fulfilled its obligations to make reasonable inquiries about whether CSIS has material that should be disclosed to the accused.

Recommendation 14:

There is no need for further legislation governing the production for a criminal prosecution of intelligence held by CSIS. The procedures available under section 38 of the *Canada Evidence Act* provide an appropriate and workable framework for the trial court to determine whether production of such intelligence is warranted.

---

77 2009 SCC 3 at para. 49.

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

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

6.0 Introduction

Evidentiary privileges are complex rules developed by the courts to keep information which is valued by society confidential. The best known privilege is the one ensuring the confidentiality of information that passes between lawyers and their clients during the provision of legal advice. The disclosure requirements in *Stinchcombe* do not apply to material covered by evidentiary privileges. This important limit is not always fully understood.

Another important privilege is the "police informer privilege." This privilege protects all identifying information about an informer who has supplied the police with information in exchange for a promise of secrecy and anonymity. The privilege is designed both to protect informers who provide information under a promise of anonymity and to encourage others to come forward with information.

Police informer privilege is a "class," or "absolute," privilege because it protects information without any need to balance the competing interests in disclosure and non-disclosure. The police informer privilege binds police, prosecutors and judges, and cannot be waived unilaterally by the Crown. The privilege can be waived only with the informer's consent. It effectively gives an informer a veto about being called as a witness. An exception to police informer privilege is allowed when such information is the only means to establish the innocence of an accused.[1] Another class privilege at the federal level is that applying to all Cabinet confidences.[2]

Class privileges can be contrasted with "qualified" privileges, which involve balancing the interests in disclosure and non-disclosure, while taking into account the facts of the particular case.[3] Class privileges offer maximum advance certainty that the information covered by the privileges will not be disclosed.

---

1 *Named Person v. Vancouver Sun*, 2007 SCC 43, [2007] 3 S.C.R. 252.
2 *Canada Evidence Act*, R.S.C. 1985, c. C-5, s. 39 [*Canada Evidence Act*].
3 Qualified privileges under the *Canada Evidence* Act, such as specified public interest immunity privilege (s. 37) and national security privilege (s. 38), are examined in Chapter VII.

The police informer privilege creates a tension between competing demands for secrecy and for disclosure. The stakes are high. On the one hand, a promise of anonymity to an informer may be necessary to obtain information that is vital for preventing terrorism. On the other hand, such a promise may make terrorism prosecutions more difficult, if not impossible, by giving the informer a virtual veto over whether he or she will testify in support of the prosecution case.

The police informer privilege does not extend to individuals who act as state agents or who become material witnesses to a crime – a frequent occurrence in terrorism investigations, where the best informers often play an active role or become witnesses to crimes.

It is not clear whether CSIS informers are protected by police informer privilege at all, or even whether they can be protected by the privilege if responsibility for their "handling" is transferred to the RCMP.

The proper management of informers, which includes making informed decisions about when the public interest warrants promises to informers that may produce a finding of police informer privilege, is essential for the success of terrorism investigations and prosecutions.

The first part of this chapter focuses on the important, but uncertain, role played by police informer privilege in terrorism investigations. Later, the chapter examines the case for recognizing a new class privilege to protect the deliberations of the National Security Advisor (NSA). This privilege would be designed to offer maximum certainty that information shared with the NSA, as well as the deliberations within the NSA's office, would be protected against compelled disclosure. The goal would be to give the NSA a "zone of confidentiality" that would allow the NSA to discharge the additional responsibilities that are recommended in Chapter II without fear of publicity. The privilege would facilitate the sharing of information, central coordination, dispute resolution and central oversight that are necessary to ensure the effectiveness of Canada's national security activities.

6.1 The Role of Police Informer Privilege in Terrorism Investigations and Prosecutions

Despite the importance of the police informer privilege, its precise parameters are not clear. The jurisprudence does not provide definitive answers to basic questions such as the point at which the privilege is established and whether it applies to CSIS informers.

It is important to know whether CSIS informers can benefit from informer privilege, either because of their relationship with CSIS or because of promises made by the RCMP if handling of the informer is transferred to the RCMP. The answer to this question will determine the extent to which both agencies can protect the informers they handle. Potential informers may refuse to provide

information, including information that may be vital for preventing a deadly terrorist act, unless they are promised anonymity and they are confident that they will not be compelled to testify.

The prosecution of Talwinder Singh Parmar and others for an alleged conspiracy to commit terrorist acts in India collapsed in 1987 when an informer did not agree to have identifying information disclosed or to enter a witness protection program.[4] Informers may be inclined to rely on informer privilege and may refuse to testify if they view witness protection programs as inadequate.

In another case, a conviction for a conspiracy to blow up an Air India aircraft in 1986 was overturned, and a stay was eventually entered, because of the unwillingness of the police to reveal the identity of an informer known as "Billy Joe." The courts held that this individual was not protected by informer privilege because the individual had acted as an active agent of the state and was a material witness to the alleged terrorist conspiracy.[5]

Informers who get too close to terrorist plots may lose the benefits of informer privilege by acting as a police agent or by becoming a material witness to terrorist crimes.[6] Losing the protection of the privilege can have dramatic consequences for the informer. The informer's identity may be disclosed in court and the informer might be compelled to be a witness. In some cases, the safety of the informer and that of the informer's family may be threatened, or other forms of intimidation may occur. Adequate witness protection programs are therefore essential. These programs are examined in Chapter VIII.

The authority of police officers to make enforceable promises of anonymity to informers has long been recognized as an important tool for law enforcement. The Supreme Court of Canada recently remarked on this in *Named Person v. Vancouver Sun*:

> Police work, and the criminal justice system as a whole, depend to some degree on the work of confidential informers. The law has therefore long recognized that those who choose to act as confidential informers must be protected from the possibility of retribution. The law's protection has been provided in the form of the informer privilege rule, which protects from revelation in public or in court of the identity of those who

---

4 *R. v. Parmar* (1987), 31 C.R.R. 256 (Ont. H.C.J.), discussed in Kent Roach, "The Unique Challenges of Terrorism Prosecutions: Towards a Workable Relation Between Intelligence and Evidence" in Vol. 4 of Research Studies: The Unique Challenges of Terrorism Prosecutions, pp. 103-111 [Roach Paper on Terrorism Prosecutions].

5 *R. v. Khela* (1998), 126 C.C.C. (3d) 341 (Que. C.A.), discussed in Roach Paper on Terrorism Prosecutions, pp. 157-165.

6 For arguments that the most useful informers are "active" and that they may be subject to claims of entrapment and attacks on their credibility, see Jean-Paul Brodeur, "The Royal Canadian Mounted Police and the Canadian Security Intelligence Service: A Comparison Between Occupational and Organizational Cultures" in Vol. 1 of Research Studies: Threat Assessment RCMP/CSIS Co-operation, pp. 207-208.

> give information related to criminal matters in confidence. This protection in turn encourages cooperation with the criminal justice system for future potential informers.[7]

The Court stressed the breadth of the privilege, noting that "… [a]ny information which might tend to identify an informer is protected by the privilege. The protection is not limited simply to the informer's name, but extends to any information that might lead to identification." The privilege imposes a duty on the police, the Crown, lawyers and judges "…to keep an informer's identity confidential."[8]

The Supreme Court states that "… [p]art of the rationale for a mandatory informer privilege rule is that it encourages would-be informers to come forward and report on crimes, safe in the knowledge that their identity will be protected."[9] Unlike a case-by-case confidentiality privilege or public interest immunity, or national security confidentiality privileges determined under sections 37 and 38 of the *Canada Evidence Act*[10], the police informer privilege is absolute, once it is found to exist, subject only to the innocence-at-stake exception:

> Informer privilege is of great importance. Once established, the privilege cannot be diminished by or 'balanced off against' other concerns relating to the administration of justice. The police and the court have no discretion to diminish it and are bound to uphold it.[11]

In contrast, in making a claim to a privilege by using section 38 of the *Canada Evidence Act*, the Attorney General of Canada must demonstrate that the disclosure of the information would harm national security, national defence or international relations. Moreover, the judge must determine whether the harm in that case of disclosing secret information outweighs the harm of not disclosing it.

Police informer privilege has been recognized in several situations involving national security. The Supreme Court held that the privilege extends even to police intelligence work involving confidential health records, and when the investigation is not tied to any particular prosecution. In *Solicitor General of Canada v. Royal Commission (Health Records)*, Martland J. stated for the Court that the foundation of the police informer privilege "…is even stronger in relation to the function of the police in protecting national security":

---

7 2007 SCC 43, [2007] 3 S.C.R. 252 at para. 16.
8 2007 SCC 43, [2007] 3 S.C.R. 252 at para. 26.
9 *Named Person v. Vancouver Sun*, 2007 SCC 43, [2007] 3 S.C.R. 252 at para. 39.
10 R.S.C. 1985, c. C-5.
11 *R. v. Leipert*, [1997] 1 S.C.R. 281 at para. 28.

> The rule of law which protects against the disclosure of informants in the police investigation of crime has even greater justification in relation to the protection of national security against violence and terrorism.[12]

These comments were made in 1981. The subsequent bombing of Air India Flight 182 and the 9/11 attacks further underscored the importance of the state interest in obtaining information about terrorist suspects and in preventing terrorist acts. The ability of the police to rely on informer privilege to obtain such information is of supreme importance, even if the privilege may make it much more difficult to conduct certain terrorism prosecutions.

In 1983, the Supreme Court stated in *Bisaillon v. Keable*[13] that informer privilege and "Crown privilege" – which today might be called national security confidentiality privilege under section 38 of the *Canada Evidence Act* – are both rooted in the fact that secrecy is sometimes in the public interest.

6.1.1 Loss of Informer Privilege When the Informer Is or Becomes an Agent or Material Witness

The police informer privilege does not apply when the police informer is or becomes an agent acting for the state or a material witness to the alleged crime. This is simply because the accused's right in these situations to make full answer and defence becomes more important than protecting the informer's identity. This qualification of the police informer privilege is especially relevant in terrorism investigations because informers who become privy to a secret terrorist plot may often be material witnesses to the plot, act as state agents in trying to foil the plot, or both.

The limits of the police informer privilege were revealed in a terrorism prosecution that stemmed from an alleged conspiracy to blow up an Air India aircraft in 1986. The Quebec Court of Appeal held that the identity of the informer "Billy Joe" was not protected by police informer privilege because the informer had become a material witness. The informer's testimony was relevant to whether a crime had been committed and to whether the accused had an entrapment defence.[14] This prosecution was eventually stayed by the courts because of persistent non-disclosure by the Crown of the informer's identity and of other information, including notes from police interviews with the informer.[15] This case demonstrates how restrictions on the police informer privilege designed to protect the accused's right to a fair trial can make terrorism prosecutions and the protection of informers difficult. When an informer's identity must be revealed because the informer has become a material witness or state agent, the prosecution has only two options: provide

---

12 *Solicitor General of Canada, et al. v. Royal Commission (Health Records)*, [1981] 2 S.C.R. 494 at 537.
13 [1983] 2 S.C.R. 60.
14 *R. v. Khela* (1991), 68 C.C.C. (3d) 81 (Que. C.A.).
15 *R. v. Khela* (1998), 126 C.C.C. (3d) 341 (Que. C.A.).

partial anonymity and adequate witness protection for the informer, or abandon the prosecution. The adequacy of witness protection programs, as well as "partial anonymity" devices that allow those like "Billy Joe" to be identified only by false names or to testify in court by means of video links or behind screens,[16] are examined in Chapter VIII.

Promises of anonymity that are not kept erode the trust between informers and the authorities and may lead informers to switch stories or have "memory lapses" when asked to testify. Generally, it is best for security intelligence and police agencies to be honest with informers about the possible disclosure of their identities and the possible need for them to testify if they become material witnesses or agents.

The authorities should also be given the means to address informers' safety concerns. When necessary, both police and security intelligence agencies should have access to flexible witness protection programs.

In many cases, disruption of a terrorist plot should take priority over a subsequent prosecution for the resulting terrorist act, and it may be necessary to promise anonymity to achieve this. Such promises should not, however, be made routinely. It must be remembered that a promise, if honoured, may make a subsequent prosecution difficult, if not impossible. In general, individual officers or agents should not have the sole discretion to decide whether to promise anonymity. Procedures should be established to allow consideration of all the available evidence. There must be sound decision making and respect for the chain of command within organizations.

The reliability of the informer should be one factor to consider in offering anonymity, because an unreliable informer might change his or her story, yet remain protected by informer privilege. Legal advice should be obtained, whenever possible, both about the legal effects of promises made to informers and about the impact on subsequent prosecutions of granting informer privilege. Legal advice will also be necessary to determine whether an informer may have already lost, or is likely to lose, the benefit of informer privilege because he or she has become an agent or a material witness.

In some cases, protecting an informer through a witness protection program might be offered as an alternative to a grant of police informer privilege.

Recommendation 15:

The RCMP and CSIS should each establish procedures to govern promises of anonymity made to informers. Such procedures should be designed to serve the public interest and should not be focused solely on the mandate of the particular agency.

---

16 *Criminal Code*, R.S.C. 1985, c. C-46, s. 486.2(4)-(5).

6.2 Informer Privilege and the Transfer of Sources from CSIS to the RCMP

In a pre-trial ruling during the Air India trial, Justice Josephson held that CSIS was subject to *Stinchcombe* disclosure requirements. He added:

> …[T]he submission that the Witness should be characterized as a confidential informant subject to informer privilege is contrary to all of the evidence in relation to her treatment by C.S.I.S. While it is not necessary to determine whether in law C.S.I.S. can cloak a source with the protections of informer privilege, it is clear that its subsequent actions in passing the Witness's information and identity to the R.C.M.P. suggest that it never regarded or treated her as such.[17]

Although this comment was not strictly necessary for the judgment, the comment would mean that any chance that a source could be protected by informer privilege would be lost whenever CSIS passed information about a source to the police under section 19(2)(a) of the *CSIS Act*[18]. Because CSIS has a statutory duty to ensure the secrecy of its sources, it might therefore be reluctant to share information about its sources with the RCMP.

Chapter IV recommended that CSIS should no longer have a discretion under section 19(2)(a) to withhold information that is relevant to police investigations or prosecutions. For this recommendation to work, it would be necessary to allow CSIS to pass information about a source to the RCMP or to the NSA without the source losing the possibility of obtaining informer privilege. This does not mean that informer privilege should be promised in every case or that CSIS officials should be permitted by law to make promises that will result in informer privilege. Nevertheless, there must be a mechanism that allows information about informers to be shared between CSIS and the RCMP, or between CSIS and the NSA, without losing the possibility of claiming informer privilege.

Information sharing between CSIS and the RCMP should be a two-way flow. In some cases, the RCMP might wish to tell CSIS about one of its informers without losing the possibility of informer privilege.

Some courts have indicated that information can be shared among the police and with Crown counsel without losing informer privilege. In one case, a judge held that police informer privilege was preserved even though the identity of the informer had been revealed to three members of the RCMP, one member of the OPP, two judges, a court registrar, a lawyer in private practice working for the federal Department of Justice and a federal prosecutor. The judge commented:

---

17 *R. v. Malik and Bagri*, 2004 BCSC 554, 119 C.R.R. (2d) 39 at para. 18.
18 R.S.C. 1985, c. C-23.

> Since police officers, judges and Crown attorneys routinely share information subject to the privilege, it is clear that such information can be shared in a limited way without breach of the guarantee and without the consent of the informer. In fact, the circle of people entitled to share the information expands over time, and is dependant on the facts. The expansion of this circle occurs without breach of the guarantee, without the consent of the informer and, most importantly, without violating the policy upon which the privilege is founded. The Crown attorney in this application, for example, may have to modify the presentation of his case in order to respect the privilege.[19]

The claim of police informer privilege was upheld on appeal. As a result, the RCMP Public Complaints Commission (since renamed the Commission for Public Complaints Against the RCMP) did not gain access to the informer's identity. However, Justice Létourneau expressed concern about the number of people with access to the informer's identity:

> Safety and secrecy are major preoccupations surrounding police informer privilege. I confess that I am deeply troubled by the number of persons who had access to the privileged information in this case, thereby increasing the risk of disclosure and of defeating the purpose of the privilege. If potential informers were made aware of the way information was shared in this instance, I am not sure that many of them would be keen on coming forward in the future. Furthermore, the fact that information may have been improperly shared in this case cannot serve as support for the appellant's position. To add the Chairperson of the Commission and some of her staff to an already long list would be to add persons who are interested in accessing the privileged information in order "to ensure the highest possible standard of justice". However, as laudable as this goal may be, it cannot justify granting access to persons who are not persons who need to know such information for law enforcement purposes as required in the context of police informer privilege: see *Bisaillon*. I am persuaded that, if consulted, informers would, for safety reasons, strongly oppose the opening of an additional circuit of distribution of their names, especially where the justification for this distribution is the furtherance of a purpose other than that of law enforcement in the strict sense.[20]

---

19 *Canada (Royal Canadian Mounted Police Public Complaints Commission) v. Canada (Attorney General)*, 2004 FC 830, 255 F.T.R. 270, Arguments at para. 20.

20 *Canada (Royal Canadian Mounted Police) v. Canada (Attorney General)*, 2005 FCA 213, 256 D.L.R. (4th) 577 at para. 46.

Justice Létourneau held that "…in the context of the police informer privilege, the notion of 'Crown' should be narrowly defined and refers to those persons who are directly involved in the enforcement of the law,"[21] and, as such, did not include the RCMP Public Complaints Commission.

This decision raises the issue of whether, for the purpose of claiming informer privilege, the "Crown" would include CSIS. Although it could be argued that CSIS is not "…directly involved in the enforcement of the law," such a conclusion would be unrealistic and impractical in the context of terrorism investigations. CSIS, unlike the Commission for Public Complaints, plays a vital role in terrorism investigations and has statutory obligations to protect the identity of its sources. Section 19(2)(a) of the *CSIS Act* should be amended to make it clear that information about an individual which is exchanged by CSIS with a police force or with the NSA does not prejudice a claim of informer privilege.

Recommendation 16:

Section 19 of the *CSIS Act* should be amended to provide that information about an individual which is exchanged by CSIS with a police force or with the NSA does not prejudice claiming informer privilege.

6.3 Should CSIS Informers Be Protected by Informer Privilege

The courts have not yet given clear guidance about whether promises of anonymity by CSIS to its informers create police informer privilege. In the pre-trial ruling discussed earlier, Justice Josephson did not decide whether CSIS could cloak its human sources with informer privilege.[22] He simply held that the actions of CSIS in disclosing an informer's identity and information to the RCMP were inconsistent with any subsequent claim of informer privilege. For the reasons set out above, the idea that the transfer of information between CSIS and the police would not permit subsequent claims of informer privilege is unworkable and should be rejected.

Canadian courts have generally been reluctant to extend informer privilege beyond the law enforcement context. In *Reference re Legislative Privilege*,[23] the Ontario Court of Appeal refused to extend informer privilege to whistleblowers who contacted members of the legislature. In the United Kingdom, however, there has been a willingness to extend the privilege to those who assist public authorities to uncover wrongdoing such as abuse of children[24] and gaming

---

21 2005 FCA 213, 256 D.L.R. (4th) 577 at para. 43.
22 *R. v. Malik and Bagri*, 2004 BCSC 554, 119 C.R.R. (2d) 39.
23 (1978) 39 C.C.C. (2d) 226 (Ont. C.A.).
24 *D. v. National Society for the Prevention of Cruelty to Children*, [1978] A.C. 171 (C.A.).

frauds.[25] Colin Gibbs, a Crown prosecutor from the United Kingdom, testified that the informer privilege applies to sources for UK intelligence services.[26]

In a recent case involving an unsuccessful attempt by special advocates to cross-examine human sources in a security certificate case, Federal Court Justice Noël concluded that the police informer privilege did not apply to CSIS human sources. He reasoned:

> The covert human intelligence source(s) at issue in this motion for production are recruited by a civilian intelligence agency; they are not "police" informers providing information to police in the course of their duties.... Covert human intelligence sources are individuals who have been promised confidentiality in return for their assistance in gathering information relating to the national security concerns of Canada. Thus the common law privilege protecting police informers and the innocence at stake exception to that privilege are not applicable *per se* to the covert human intelligence sources recruited by the Service.[27]

Although he concluded that the privilege did not apply to CSIS sources, Justice Noël nevertheless found that the sources were protected on the basis of a case-by-case confidentiality privilege because of the great importance of confidentiality and the injury to national security that could be caused by revealing the identity of CSIS sources.[28] He stressed that "…[c]onfidentiality guarantees are essential to the Service's ability to fulfill its legislative mandate to protect the national security of Canada while protecting the source from retribution."[29] The CSIS informer privilege that he recognized was, however, not as protective as police informer privilege, which is limited only by the innocence-at-stake exception and by the fact that it does not apply in non-criminal proceedings. The new CSIS informer privilege would be subject to a "need-to-know" exception that would apply if there was no other way to "…establish that the proceeding will otherwise result in a flagrant denial of procedural justice which would bring the

---

25 *Rogers v. Home Secretary; Gaming Board for Great Britain v. Rogers*, [1973] A.C. 388 (H.L. (E.)). In a 1977 deportation case, Lord Denning held "…[t]he public interest in the security of the realm is so great that the sources of the information must not be disclosed, nor should the nature of the information itself be disclosed, if there is any risk that it would lead to the sources being discovered. The reason is because, in this very secretive field, our enemies might try to eliminate the source of information. So the sources must not be disclosed. Not even to the House of Commons. Nor to any tribunal or court of inquiry or body of advisers, statutory or non-statutory, save to the extent that the Home Secretary thinks safe": *R. v. Secretary of State for the Home Department, ex parte Hosenball* [1977] 3 All ER 452 at 460 (C.A.). Geoffrey Lane similarly stated that "…once a potential informant thinks that his identity is going to be disclosed if he provides information, he will cease to be an informant. The life of a known informant may be made, to say the least, very unpleasant by those who, for reasons of their own, wish to remain in obscurity": at 462.

26 Testimony of Colin Gibbs, vol. 84, November 28, 2007, pp. 10812-10813.

27 *Harkat (Re)*, 2009 FC 204 at para. 18.

28 2009 FC 204 at paras. 27-29.

29 2009 FC 204 at para. 31.

administration of justice into disrepute."[30] This exception could arise "…where, in the judge's opinion, there is no other way to test the reliability of critical information provided by a covert human intelligence source except by way of cross-examination."[31]

Whether Canadian courts might one day recognize a police informer privilege for CSIS informers is impossible to know. There are strong arguments both for and against finding the existence of the privilege in such circumstances. The following are arguments against extending the privilege to CSIS informers:

- Parliament made a decision not to give CSIS law enforcement powers. The informer privilege, at least in Canada, has traditionally been reserved for police informers;
- CSIS deals with informers under its mandate to investigate threats to the security of Canada. It will often be premature at the time of such investigations to make promises that effectively give informers a veto over whether they can be called as witnesses or whether any identifying information about them is disclosed in a subsequent terrorism prosecution;
- The identities of CSIS sources can already be protected through applications for public interest immunity and national security confidentiality under sections 37 and 38 of the *Canada Evidence Act* or through the recognition of a case-by-case privilege. CSIS dealings with its sources would fall under the first three Wigmore criteria: (1) the communications originated in a confidence that they will not be disclosed; (2) the confidentiality is essential to the maintenance of the relation between the parties; and (3) the relation is one that should be fostered.[32] The critical question in most cases would be whether the injury to the relation by disclosure of the communication would be greater than the benefit gained for the correct disposal of litigation;

---

30 2009 FC 204 at at para. 61.
31 2009 FC 204 at para. 46.
32 *R. v. Gruenke*, [1991] 3 S.C.R. 263.

- Extending informer privilege to CSIS informers is not necessary because section 18 of the *CSIS Act* makes it an offence punishable by up to five years imprisonment to disclose information about a confidential source of information or assistance to CSIS. However, this protection, unlike informer privilege, does not bind courts when they make disclosure orders;[33] and
- Extending police informer privilege to CSIS sources might lead to judges weakening the protections of informer privilege by gradually allowing the privilege to be defeated by exceptions in addition to the existing innocence-at-stake exception.

On the other hand, there are several arguments in favour of extending the privilege to CSIS informers:

- Although CSIS does not have law enforcement powers, there is often a close nexus between CSIS investigations of threats to security and terrorist crimes, treason, espionage and violations of the *Security of Information Act;*[34]
- It may be contrary to the public interest to allow a police officer to make enforceable promises of anonymity to obtain information about what may only be minor crimes, while a CSIS agent could not make similar promises even where the promises might be needed for the agent to obtain information about an imminent terrorist act;
- Better coordination of CSIS and RCMP counterterrorism investigations may reduce the risk that CSIS promises would prematurely trigger a police informer privilege;
- As a class privilege subject only to the innocence-at-stake exception, informer privilege provides greater protection for the identity of informers than the protections now available to CSIS sources under section 18 of the *CSIS Act* and sections 37 and 38 of the *Canada Evidence Act,* or under a confidentiality privilege recognized under common law; and
- Current CSIS practice seems to be to give human sources "… absolute promises that their identity will be protected,"[35] and such promises encourage sources to provide information relating to security threats.

---

33 Section 18(2) of the *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23 provides that a person may disclose information about a person who is or was a confidential source of information or assistance to CSIS "…for the purposes of the performance of duties and functions under this Act or any other Act of Parliament or the administration or enforcement of this Act or as required by any other law or in the circumstances described in any of paragraphs 19(2)(*a*) to (*d*)." Section 19(2)(a) in turn allows disclosure of information "…where the information may be used in the investigation or prosecution of an alleged contravention of any law of Canada or a province, to a peace officer having jurisdiction to investigate the alleged contravention and to the Attorney General of Canada and the Attorney General of the province in which proceedings in respect of the alleged contravention may be taken".

34 R.S.C. 1985, c. O-5.

35 *Harkat (Re)*, 2009 FC 204 at para. 31.

CSIS generally sees promises of anonymity to its sources as essential to obtain their cooperation. As Justice Noël recently stated, such promises "…not only foster long-term, effective relationships with the sources themselves, but increase, exponentially, the chances for success of future intelligence investigations. Confidentiality guarantees…also [encourage] others to come forward with essential information that would not otherwise be available to the Service."[36]

Given the preventive nature of CSIS counterterrorism investigations and their use during the early stages of suspicious activities, CSIS may have difficulty determining whether its investigations will later uncover criminal behaviour that would warrant police investigation and criminal prosecution. CSIS promises of anonymity to human sources might often be premature and could, if the promises were enforceable, jeopardize subsequent terrorism prosecutions. Yet, given its mandate, CSIS will have a strong incentive to make promises to sources that will assist it to collect intelligence, and much less incentive to help make sources available to testify in a terrorism prosecution. Indeed, the available public evidence suggests that CSIS gives "covert human intelligence sources" absolute promises that their identities will be protected.[37]

The Commission does not recommend that police informer privilege be extended by statute to CSIS informers. However, if police informer privilege is extended by statute or by the common law to CSIS informers, there must be even greater integration of CSIS and RCMP counterterrorism investigations, and the proposed Director of Terrorism Prosecutions[38] must advise both agencies about the impact of promises of anonymity on subsequent terrorism prosecutions.

In some cases, it will be necessary to make enforceable promises of anonymity to a source to obtain information that may prevent an act of terrorism, but such promises should not become routine. Rather, they should be made only in the public interest and on the basis of the most complete information available.

In the absence of a clear judicial decision that CSIS informers can be protected by police informer privilege, closer cooperation between CSIS and the RCMP and a change to the *CSIS Act* may achieve the same effect. The *CSIS Act* should be amended to allow CSIS to transfer the handling of a human source to the RCMP or other police force while preserving the ability of the police to make promises that will trigger police informer privilege.

Recommendation 17:

CSIS should not be permitted to grant police informer privilege. CSIS informers should be protected by the common law "Wigmore privilege," which requires the court to balance the public interest in disclosure against the public interest in confidentiality. If the handling of a CSIS source is transferred to the RCMP, the source should be eligible to benefit from police informer privilege.

---

36 *Harkat (Re)*, 2009 FC 204 at para. 31.
37 *Harkat (Re)*, 2009 FC 204 at para. 31.
38 The role of the proposed Director of Terrorism Prosecutions is discussed in Chapter III.

6.4 Are New National Security Privileges Necessary

The modern trend has been away from class (absolute) privileges that promote secrecy over disclosure. For example, the Supreme Court of Canada has refused to recognize a new class privilege that would apply to religious communications[39] or that would apply to private therapeutic records.[40] In the latter case, Justice L'Heureux-Dubé explained this reluctance:

> Generally, class privilege presents many impediments to the proper administration of justice and, for that reason, has not been favoured in Canada and elsewhere in criminal trials. A class privilege is a complete bar to the information contained in such records, whether or not relevant, and the onus to override it is a heavy one indeed. The particular concerns raised by the recognition of a class privilege in favour of private records in criminal law relate to: (1) the truth-finding process of our adversarial trial procedure; (2) the possible relevance of some private records; (3) the accused's right to make full answer and defence; (4) the categories of actors included in a class privilege; and (5) the experience of other countries.[41]

The Court did not create a new class privilege to protect therapeutic records from disclosure. The Court recognized that class privileges provide the greatest certainty against disclosure, but that they also can inhibit the truth-seeking function of the criminal trial and impair the accused's right to make full answer and defence.

In 1982, the Supreme Court upheld a class privilege that prevented the disclosure of information whenever a minister of the Crown certified that the disclosure of a document "…would be injurious to international relations, national defence or security, or to federal-provincial relations"[42] or would disclose a Cabinet confidence. The Court based its ruling on "parliamentary supremacy."[43] The case was decided without referring to the *Charter* and despite the fact that the British common law had evolved away from absolute privileges, even in the national security context.[44] Parliament soon repealed the Canadian absolute privilege, in part because of concerns that it would be found to be inconsistent with the *Charter*. In subsequent years, even established class privileges, such as the informer privilege[45] and solicitor and client privilege,[46] have been subject to

---

39 *R. v. Gruenke*, [1991] 3 S.C.R. 263.
40 *A. (L.L.) v. B. (A.)*, [1995] 4 S.C.R. 536.
41 [1995] 4 S.C.R. 536 at para. 65.
42 *Federal Court Act*, R.S.C. 1970 (2nd Supp.), c. 10, s. 41(2).
43 *Commission des droits de la personne v. Attorney General of Canada*, [1982] 1 S.C.R. 215 at 228.
44 The absolute approach taken in *Duncan v. Cammell, Laird & Co., Ld.*, [1942] A.C. 624 (H.L. (E.)) should be compared with the more flexible approach contemplated in *Conway v. Rimmer*, [1968] A.C. 910 (H.L. (E.)).
45 *R. v. Leipert*, [1997] 1 S.C.R. 281.
46 *R. v. McClure*, 2001 SCC 14, [2001] 1 S.C.R. 445.

innocence-at-stake exceptions. Such exceptions ensure that the privileges are consistent with the *Charter* and, in particular, with the accused's right to make full answer and defence.

6.4.1 Cabinet Confidences

One exception to the trend away from absolute privileges is that attaching to Cabinet deliberations. In *Babcock v. Canada*, the Supreme Court of Canada upheld the constitutionality of section 39 of the *Canada Evidence Act*, which provides that the disclosure of Cabinet confidences must be refused "…without examination or hearing of the information by the court, person or body," upon certification by the Clerk of the Privy Council or by a minister. The Court articulated the rationale for this broad class privilege in the following terms:

> Those charged with the heavy responsibility of making government decisions must be free to discuss all aspects of the problems that come before them and to express all manner of views, without fear that what they read, say or act on will later be subject to public scrutiny....[47]

The Court stated that section 39 of the *Canada Evidence Act* contained "absolute language" that "…goes beyond the common law approach of balancing the public interest in protecting confidentiality and disclosure on judicial review. Once information has been validly certified, the common law no longer applies to that information."[48]

Despite the absolute language in section 39, the Court held that the certification of a document as a Cabinet confidence would have to be done for the "…*bona fide* purpose of protecting Cabinet confidences in the broader public interest."[49] A certification would be invalid if done for purposes not authorized by the legislation or if it related to information that had previously been disclosed.[50] When interpreted in this manner, section 39 does not infringe constitutional principles relating to the separation of powers and the independence of the judiciary.[51] It provides a broad, but not unlimited, protection for Cabinet confidences.

---

47 *Babcock v. Canada (Attorney General)*, 2002 SCC 57, [2002] 3 S.C.R. 3 at para. 18.
48 2002 SCC 57, [2002] 3 S.C.R. 3 at para. 23.
49 2002 SCC 57, [2002] 3 S.C.R. 3 at para. 25.
50 2002 SCC 57, [2002] 3 S.C.R. 3 at paras. 25-26.
51 The Court explained that "…s. 39 has not substantially altered the role of the judiciary from their function under the common law regime. The provision does not entirely exclude judicial review of the determination by the Clerk that the information is a Cabinet confidence. A court may review the certificate to determine whether it is a confidence within the meaning provided in s. 39(2) or analogous categories, or to determine if the certificate was issued in bad faith. Section 39 does not, in and of itself, impede a court's power to remedy abuses of process": 2002 SCC 57, [2002] 3 S.C.R. 3 at para. 60.

6.4.2 A New National Security Privilege for Deliberations of the National Security Advisor

Statutory recognition should be given to a new national security privilege. Following the model of Cabinet confidentiality under section 39 of the *Canada Evidence Act*, this new national security privilege would extend only to material prepared to assist the deliberations of the NSA and to material that recorded the NSA's deliberations.

The new privilege would not protect material already held by CSIS, the RCMP or other agencies if that material was not specifically prepared for the NSA. It would also not protect material prepared by these agencies after a decision by the NSA or after the NSA disclosed the information onwards.

The privilege would also apply to work done by the NSA to evaluate and oversee the effectiveness of Canada's national security activities and systems. This would help to ensure that gaps in Canada's security were not publicized while remedial steps were being taken to close them.

The justification for this new privilege might in some respects be even stronger than that for privileges related to Cabinet confidences. The privilege relating to the NSA would be justified by the need to promote candour in discussions and because all the material covered by the privilege would relate to national security. Under the proposed amendments to section 19 of the *CSIS Act* discussed in Chapter IV, CSIS would submit to the NSA only the intelligence that CSIS believed should not be disclosed to the police – for example, intelligence relating to particularly sensitive ongoing national security investigations.

The NSA would also produce and receive material that was relevant to the oversight of national security activities and that might reveal gaps and weaknesses in security systems. The new privilege would give the NSA the freedom to receive the broadest range of candid views and consider the greatest range of options. Because the privilege would not apply to original materials held by the various agencies, including CSIS and the RCMP, or to material disclosed by the NSA, intelligence that would be disclosed to the police would not be shielded by the privilege. This would protect an accused's right to disclosure and to make full answer and defence. However, sections 37 or 38 of the *Canada Evidence Act* could still be used to try to prevent intelligence that has been given to the police from being disclosed.

The new national security privilege should apply once the Clerk of the Privy Council certifies that the information relates to confidences that were shared with the NSA or to deliberations of the NSA. As under the 2002 Supreme Court of Canada decision in *Babcock*,[52] judicial review would be possible, but only on narrow grounds. Judicial review would be permitted if the information had

---

52 *Babcock v. Canada (Attorney General)*, 2002 SCC 57, [2002] 3 S.C.R. 3.

previously been disclosed, or to address allegations that the certification was not made for a *bona fide* reason authorized by the *Canada Evidence Act*.

The new privilege should not apply if it was determined that the accused's innocence was at stake and if there was no other manner to obtain the information.[53] It is unlikely, however, that this situation would arise, because the privilege would not apply to information that the NSA disclosed to police or prosecutors. The normal rules of disclosure dictated by *Stinchcombe* for material held by the Crown, and by *O'Connor* for material held by CSIS, would apply.[54]

Any attempt to secure access to the deliberations of the NSA would require the Attorney General of Canada to invoke the national security confidentiality provisions of section 38 of the *Canada Evidence Act*. For this reason, only courts that have jurisdiction under section 38 should have the ability to determine whether the conditions of this new privilege are satisfied.[55] This limitation should not thwart the important work of SIRC because it would still have full access to information held by CSIS.

Even if no new privilege is legislated, material prepared for the NSA and the deliberations of the NSA would likely be protected from disclosure under the national security confidentiality provisions in section 38 of the *Canada Evidence Act*. Most of the information prepared for and produced by the NSA has a strategic and policy character. For this reason, it is unlikely that a court would conclude that the information has a significant benefit for the correct disposal of litigation. As a result, it would be very unlikely that the court would order the material disclosed. Even so, a new class privilege is necessary to provide maximum certainty to CSIS, and to other agencies providing information to the NSA, that the information will not be subject to disclosure.

Recommendation 18:

The *Canada Evidence Act* should be amended to create a new national security privilege, patterned on the provision for Cabinet confidences under section 39 of the Act. This new class privilege should apply to documents prepared for the National Security Advisor and to the deliberations of the office of the National Security Advisor.

---

53 *Named Person v. Vancouver Sun*, 2007 SCC 43, [2007] 3 S.C.R. 252.

54 See Chapter V for discussion of these disclosure requirements.

55 Although the Supreme Court has not decided this issue, it has suggested that all bodies with jurisdiction to compel the production of information would also be able to determine whether a s. 39 claim is valid: *Babcock v. Canada (Attorney General)*, 2002 SCC 57, [2002] 3 S.C.R. 3 at paras. 42-43.

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

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

7.0 Introduction

The legislative limits on disclosure and the privileges discussed in the previous two chapters are general limits on disclosure, rather than limits based on the facts of a particular case. Although general limits provide the greatest advance certainty that information will be protected from disclosure, they also run the risk of shielding too much or too little information.

New legislative limits on disclosure, or the dramatic expansion of privileges, will attract litigation. This will include *Charter* challenges claiming that the measures deprive the accused of the right to make full answer and defence, as well as litigation to help define the scope of the new provisions. The litigation will be carried out through pre-trial motions that will prolong terrorism prosecutions. Yet, even then, the core issue – whether a particular item of intelligence must be disclosed to ensure a fair trial – may not be resolved. The apparent certainty that general legislative limits on disclosure and new privileges could provide for security intelligence agencies and informers would be eroded by such litigation.

A fairer and more efficient alternative would be to improve the mechanisms for judges to review secret intelligence and to decide *on the facts of the particular case* whether the intelligence needs to be disclosed to ensure a fair trial. Such reviews are a standard and important part of terrorism prosecutions throughout the world. They recognize that police forces and intelligence agencies must work more closely to prevent terrorism, but that the disclosure of secret intelligence to the accused in a subsequent prosecution may threaten ongoing investigations, secret sources and promises of confidentiality made to allies.

However, deciding on the facts of a particular case whether to allow disclosure will produce less certainty for CSIS about whether or not its intelligence will be disclosed. As suggested in Chapter II, CSIS should be permitted to disclose sensitive intelligence to the National Security Advisor (NSA) and then to try to convince the NSA that the risk of that intelligence being disclosed through a prosecution is not acceptable.

Intelligence that is shared with the police might not always need to be disclosed to the accused in a terrorism prosecution. Under *Stinchcombe*, the Crown is required to disclose all relevant information and non-privileged information in its possession to comply with section 7 of the *Charter*, whether the information is inculpatory or exculpatory, and whether or not it is going to be presented as evidence. In some cases, the intelligence may contain material that will be valuable and perhaps even vital to the accused's defence.

Two main vehicles allow judges to make non-disclosure orders on the facts of the particular case. Section 37 of the *Canada Evidence Act*[1] allows officials to obtain a judicial non-disclosure order on the basis that the disclosure would harm a specified public interest. The protection of confidential informants and ongoing investigations might qualify here. Section 38 allows the Attorney General of Canada to obtain a judicial non-disclosure order on the basis that disclosure of the material would harm national security, national defence or international relations. In both cases, the judge must consider the competing interests in disclosure and non-disclosure. In both cases, judges can place conditions on disclosure, including partial redaction (editing) and the use of summaries and admissions of facts, in order to reconcile the competing interests in disclosure and secrecy.

In 2001, the *Anti-terrorism Act*[2] amended sections 37 and 38 of the *Canada Evidence Act*. These amendments attempted to encourage the pre-trial resolution of disputes about disclosure of sensitive information. The amendments also allowed judges to be more creative in reconciling the competing interests in disclosure and non-disclosure. Finally, the amendments gave the Attorney General of Canada a new power to issue a certificate that would block court orders to disclose material from a foreign entity or material relating to national defence or national security.[3]

Even with these amendments to the *Canada Evidence Act*, concerns remain about the workability of the procedures used to determine which material must be disclosed in a terrorism prosecution, and the form of the disclosure. For example, section 38 issues must be decided in the Federal Court even when they arise in a criminal trial before a superior court. Early in 2009, a judge in the ongoing "Toronto 18" terrorism prosecution held that the exclusive jurisdiction of the Federal Court to make decisions under section 38 about the disclosure of national security information threatens the viability of the trial process and the rights of the accused.[4]

---

1 R.S.C. 1985, c. C-5.
2 S.C. 2001, c. 41.
3 *Canada Evidence Act*, R.S.C. 1985, c. C-5, s. 38.13 [*Canada Evidence Act*].
4 Colin Freeze, "Ontario judge declares secrecy law unconstitutional," *The Globe and Mail* (January 16, 2009).

Proceedings under sections 37 and 38 occur separately from underlying criminal proceedings even if the section 37 and 38 proceedings involve questions about the information that must be disclosed to the accused. Both the accused and the Crown can appeal decisions made under sections 37 and 38 before, or even during, a terrorism trial. Such appeals have fragmented and prolonged terrorism prosecutions.

Sections 37 and 38 of the *Canada Evidence Act* are both likely to play critical roles in most terrorism prosecutions. They will be used to reconcile the competing demands for secrecy and disclosure and, as a result, the competing interests of security intelligence and law enforcement agencies. These procedures must be as efficient and fair as possible and should incorporate the best practices employed by other democracies that have had more extensive experience than Canada with terrorism prosecutions. The public needs to have confidence that Canada has sufficient competence to undertake the difficult task of prosecuting terrorism cases fairly and efficiently. As a recent report of the International Commission of Jurists stated, acts of terrorism "…are all very serious criminal offences under any legal system. If the criminal justice system is inadequate to the new challenges posed, it must be made adequate."[5]

7.1 Section 37 of the *Canada Evidence Act*

Section 37 of the *Canada Evidence Act* allows ministers or officials to ask the courts to prevent disclosure on the basis of a "specified public interest." Section 37 leaves the range of specified public interests open-ended. The interests have included the following: the protection of informers; ongoing investigations, including the location of watching posts and listening devices; the location of witnesses in witness protection programs; and investigative techniques.[6] Section 37 may be of particular importance in preventing the disclosure of information that might identify CSIS informers who are not otherwise protected by police informer privilege.

Hearings under section 37 can involve the Crown making submissions in the absence of the accused, the public, or both.[7] The Crown can also present material to the judge, even if it might not otherwise be admissible under Canadian law, as long as the material is reliable and appropriate.[8] Hearings under section 37 can consume considerable time, since they may often require submissions by the parties and judicial inspection of each disputed document.

---

5 *Assessing Damage, Urging Action: Report of the Eminent Jurists Panel on Terrorism, Counter-terrorism and Human Rights*, p. 123, online: International Commission of Jurists, Eminent Jurists Panel <http://ejp.icj.org/IMG/EJP-Report.pdf> (accesed July 30, 2009) [*Assessing Damage, Urging Action*].

6 Robert W. Hubbard, Susan Magotiaux and Suzanne M. Duncan, *The Law of Privilege in Canada* (Aurora: Canada Law Book, 2006), ch. 3.

7 *R. v. Meuckon* (1990), 57 C.C.C. (3d) 193 (B.C.C.A.); *R. v. Pilotte* (2002), 163 C.C.C. (3d) 225 (Ont. C.A.); *R. v. Pearson* (2002), 170 C.C.C. (3d) 549 (Que. C.A.).

8 *Canada Evidence Act*, s. 37(6.l).

Section 37 applications can be decided by the Federal Court or by a provincial superior court.[9] If, as with most terrorism prosecutions, the trial is held in a provincial superior court, the trial judge hears the section 37 application.[10] Section 37(5) allows the superior court judge[11] to balance the competing public interests in disclosure and non-disclosure and to make various orders relating to disclosure. The orders can include placing conditions on disclosure, such as requiring the use of a part or a summary of the information or a written admission of facts relating to the information. This is done to limit the harm to the public interest that might flow from more extensive disclosure. The judge might order material to be admitted in a modified form, such as with passages deleted, even if material altered in this way would not be admissible under ordinary rules of evidence.[12]

Under section 37.3, the trial judge can make any order that he or she considers appropriate to protect the right of the accused to a fair trial, including a stay, or termination, of all or part of the proceedings. Although a superior court trial judge is allowed to make all the relevant decisions under section 37, the *Canada Evidence Act* does not clearly state that the judge may reconsider and revise a non-disclosure order as the trial evolves.

The ability of the trial judge to reconsider and re-evaluate non-disclosure orders is critical to the efficiency and fairness of terrorism trials. A non-disclosure order that appeared appropriate at the beginning of a trial may later cause unfairness to the accused. For example, evidence introduced as the trial progresses may make it clear that information that was initially not disclosed would now greatly assist the accused. Other democracies place considerable emphasis on permitting a trial judge to re-consider an initial non-disclosure order as the trial evolves. Where appropriate, judges in Canada should also revise decisions about disclosure, using their inherent powers over the trial process.

The Crown or the accused in a criminal case can appeal a decision made under section 37 of the *Canada Evidence Act* to the provincial court of appeal,[13] with the possibility of a further appeal to the Supreme Court of Canada.[14] The Government may decide to appeal if it loses an application for non-disclosure, and the accused may do so if not satisfied by the disclosure ordered by the judge.

---

9 *Canada Evidence Act*, s. 37(3).
10 *Canada Evidence Act*, s. 37(2).
11 Provincial court trial judges do not have jurisdiction to make determinations under s. 37, but may make evidentiary rulings: *R. v. Richards* (1997), 115 C.C.C. (3d) 377 (Ont. C.A.); *R. v. Pilotte* (2002), 163 C.C.C. (3d) 225 (Ont. C.A.); *Canada (Attorney General) v. Sander* (1994), 90 C.C.C. (3d) 41 (B.C.C.A.). The division of proceedings between the provincial and superior courts in criminal proceedings may cause problems, but these are not likely to arise in terrorism prosecutions, which will generally be conducted in superior courts.
12 *Canada Evidence Act*, s. 37(8).
13 *Canada Evidence Act*, s. 37.1.
14 *Canada Evidence Act*, s. 37.2.

Because section 37 proceedings are considered to be separate from trial proceedings, the appeal rights relating to section 37 are separate from other appeals relating to the trial. The normal practice in criminal trials is to allow appeals only at the conclusion of a trial. Courts have recognized that appeal rights relating to section 37, which may be exercised before the trial is completed, can disrupt and fragment the trial.[15] If the Crown appeals a determination relating to section 37, it is possible that delay will be charged against the Crown when determining whether the accused's *Charter* right to a trial within a reasonable time has been violated.[16]

Besides appealing a determination under section 37, the Crown has other options. The Crown can stay or abandon the proceedings. As well, if an order to disclose under section 37 relates to national security or national defence, or relates to information obtained in confidence or in relation to a foreign entity, the Attorney General of Canada may personally issue a non-disclosure certificate under section 38.13 of the *Canada Evidence Act*. This power is discussed in greater detail below.

7.2 Section 38 of the *Canada Evidence Act*

A non-disclosure order can also be obtained under section 38 of the *Canada Evidence Act*. That section requires participants in proceedings to notify the Attorney General of Canada if they are required, or expect, to cause the disclosure of information that the participant believes is "sensitive information" or "potentially injurious information."[17] Once notice is given, the information cannot be disclosed unless the Attorney General of Canada or the Federal Court authorizes disclosure.[18]

A Federal Court judge, not the trial judge, must hear the matter *ex parte* and give the Attorney General of Canada the opportunity to make submissions.[19] The judge may consider material that would not ordinarily be admissible under the laws of evidence, provided that the material is reliable and appropriate.[20]

The process to decide national security confidentiality matters under section 38 has three stages. The first stage determines whether the material is relevant information that must be disclosed under *Stinchcombe*.[21] If the information is not relevant, it need not be disclosed.

---

15 *R. v. McCullough*, 2000 SKCA 147, 151 C.C.C. (3d) 281.
16 *R. v. Sander* (1995), 98 C.C.C. (3d) 564 (B.C.C.A.).
17 *Canada Evidence Act*, s. 38.01.
18 *Canada Evidence Act*, s. 38.02.
19 *Canada Evidence Act*, s. 38.11.
20 *Canada Evidence Act*, s. 38.06(3.1).
21 "The first task of a judge hearing an application is to determine whether the information sought to be disclosed is relevant or not in the usual and common sense of the Stinchcombe rule, that is to say in the case at bar information, whether inculpatory or exculpatory, that may reasonably be useful to the defence": *Canada (Attorney General) v. Ribic*, 2003 FCA 246, 185 C.C.C. (3d) 129 at para. 17.

If the information is relevant, a second stage involves determining whether the disclosure of relevant information would harm international relations, national defence or national security. In making this determination, the judge gives "considerable weight" to the submissions of the Attorney General of Canada "…because of his access to special information and expertise."[22] The judge may authorize disclosure of the information, unless he or she determines that disclosure would injure international relations, national defence or national security.[23]

If a determination is made that the disclosure of the relevant information would cause one of these harms, a third stage is involved, with the judge balancing the competing public interests in disclosure and non-disclosure.[24] The judge has a range of options. These include the authority to place conditions on disclosure, such as requiring the use of part, or a summary, of information, or a written admission of facts relating to the information, in order to limit the injury caused by the disclosure. Orders can be made to allow the admission of redacted (edited) documents, even though they would not normally be admissible under the laws of evidence.[25]

The parties may appeal a decision made under section 38 to the Federal Court of Appeal.[26] The Court is required to conduct a review if an affected party was not allowed to make representations at the section 38 hearing.[27] The Supreme Court of Canada may grant leave to appeal further.[28] These appeal and review rights treat section 38 proceedings as distinct from the trial proper, and fragment and delay criminal prosecutions.

The Attorney General of Canada may also personally issue a certificate under section 38.13 prohibiting disclosure of information that was obtained from a foreign entity or that relates to national security or national defence, even though the material is subject to a court order of disclosure. This is the ultimate protection against the disclosure of intelligence.

Section 38.131 gives a right to appeal the Attorney General's certificate, but the right is limited to determining whether the information that is the subject of the certificate in fact relates to national security or national defence or was received from, or relates to, a foreign agency.

The trial judge in any subsequent criminal trial must respect Federal Court non-disclosure orders and any non-disclosure certificate issued by the Attorney

---

22 *Canada (Attorney General) v. Ribic*, 2003 FCA 246, 185 C.C.C. (3d) 129 at paras. 18-19.
23 *Canada Evidence Act*, s. 38.06(1).
24 *Canada (Attorney General) v. Ribic*, 2003 FCA 246, 185 C.C.C. (3d) 129 at para. 21.
25 Canada Evidence Act, s. 38.06(4).
26 *Canada Evidence Act*, s. 38.09.
27 *Canada Evidence Act*, s. 38.08.
28 *Canada Evidence Act*, s. 38.1.

General of Canada. However, the trial judge has the discretion under section 38.14 to make any order that he or she considers appropriate to protect the right of the accused to a fair trial. This could include a stay of proceedings or an order dismissing specified counts of the indictment or information.

7.2.1 The Importance of Section 38 Proceedings in Terrorism Investigations and Prosecutions

Although formally characterized as separate from the criminal trial, section 38 proceedings are intimately connected to terrorism prosecutions. A 2006 Memorandum of Understanding (MOU) between the RCMP and CSIS implicitly recognizes the importance of section 38 in protecting intelligence from disclosure. It states:

The CSIS and the RCMP recognize that information and intelligence provided by the CSIS to the RCMP may have potential value as evidence in the investigation or prosecution of a criminal offence. In these cases, the parties will be guided by the following principles:

a. both parties recognize that the CSIS does not normally collect information or intelligence for evidentiary purposes;
b. both parties recognize that once information or intelligence has been disclosed by the CSIS to the RCMP, it may be deemed, for purposes of the prosecution process, to be in the control and possession of the RCMP and the Crown and thereby subject to the laws of disclosure whether or not the information is actually used by the Crown as evidence in court proceedings;
c. Sections of the *Canada Evidence Act* will be invoked as required to protect national security information and intelligence.[29]

The MOU incorrectly suggests that CSIS information and intelligence can be made subject to disclosure under *Stinchcombe* only when it is in the possession of the Crown. CSIS intelligence can, as in the Air India trial, be subject to disclosure under *Stinchcombe*. An accused can also seek production and disclosure of information from CSIS even if it is classified as a third party that is not subject to *Stinchcombe* disclosure requirements. Section 38 would be the main vehicle used to protect CSIS information, both where the accused relies on *O'Connor* to seek production and disclosure from CSIS as a third party and where the accused seeks disclosure under *Stinchcombe*.

Section 38 proceedings will be important in most terrorism prosecutions for protecting CSIS information from disclosure. Most terrorism prosecutions will feature attempts to obtain disclosure of CSIS material. Terrorism prosecutions for acts that have an international component may also see attempts to obtain

29 Public Production 1374: 2006 RCMP/CSIS MOU, Art. 21.

disclosure of material that CSIS and other Canadian agencies have obtained from foreign partners. The recently completed *Khawaja* prosecution featured multiple section 38 applications, as well as appeals to the Federal Court of Appeal and a leave application to the Supreme Court of Canada.[30]

Section 38 issues can arise at any point in a terrorism trial, with accompanying delays, especially if the accused attempts to call evidence that will involve secret intelligence, perhaps in the hope that the intelligence could exonerate the accused or cast doubt on the reliability or legality of the state's evidence. Section 38 proceedings and appeals in the middle of one criminal trial by jury led to a mistrial.[31] Concern has been expressed that mistrials could result if Federal Court proceedings become necessary in the ongoing "Toronto 18" terrorism prosecutions.[32]

7.2.2 Avoiding Section 38 Proceedings in the Air India Prosecutions

Although section 38 proceedings are likely to be a feature of contemporary terrorism prosecutions, they are not inevitable. The parties to the Air India prosecutions, for example, managed to avoid section 38 proceedings.

Reyat was convicted of manslaughter in 1991, and an appeal was dismissed in 1993.[33] Although some evidence of CSIS surveillance of Reyat and Parmar at the time of the Duncan Blast was introduced as evidence, it was not critical to the Crown's case because physical evidence was available linking Reyat to the bomb used in the Narita blast. Other incriminating evidence also existed, including admissions obtained from Reyat by the police. The Parmar Tapes that remained were disclosed to the accused without the Attorney General of Canada objecting under what is now section 38.

In the Malik and Bagri proceedings that concluded in 2005, the lawyers for the accused were given access to CSIS material, after giving an undertaking that they not disclose the evidence to others, including their clients, without permission. In a joint report on the trial, the lead prosecutor, Robert Wright, and defence counsel, Michael Code, wrote that defence counsel were able to inspect CSIS material "…while the documents remained in the possession of CSIS, and in almost every instance defence counsel were able to conclude that the material was not relevant to the proceedings."[34]

---

30 For an account of the extensive s. 38 litigation in this case, see Kent Roach, "The Unique Challenges of Terrorism Prosecutions: Towards a Workable Relation Between Intelligence and Evidence" in Vol. 4 of Research Studies: The Unique Challenges of Terrorism Prosecutions, pp. 234-245 [Roach Paper on Terrorism Prosecutions].

31 See the history leading up to the mistrial as discussed in *R. v. Ribic*, 2004 CanLII 7091 (ON S.C.) at paras. 3-9.

32 Colin Freeze, "Ontario judge declares secrecy law unconstitutional," *The Globe and Mail* (January 16, 2009).

33 *R. v. Reyat*, 1991 CanLII 1371 (BC S.C.), affirmed (1993), 80 C.C.C. (3d) 210 (B.C.C.A.).

34 Exhibit P-332: Robert Wright and Michael Code, "Air India Trial: Lessons Learned," Part III.

In his testimony before the Commission, Geoffrey Gaul, Director of the Criminal Justice Branch of the British Columbia Ministry of the Attorney General, stated that the Crown in the Malik and Bagri prosecution was prepared to litigate section 38 issues if necessary, but that it "…would have been a two-front approach"[35] that would have been "clearly daunting."[36]

Bill Turner, a senior CSIS employee, now retired, described the defence counsel undertakings not to disclose information as "a band-aid approach" that emerged from a conflict. The conflict arose because the defence wanted to explore the possibility that the Government of India was involved in the bombing, and the Government of Canada was unwilling to reveal information about "…what the Government of India is doing here in Canada….We will call it 'national security' and we wouldn't budge." Turner explained that, "…rather than go through a stay of proceedings and rather than go to Federal Court and hold the process up further," the "band-aid" solution "…was for the defence and the Crown and CSIS to sit down with all of this vetted material and CSIS would lift the vetting so the defence could look at it all and decide if they needed anything for the defence…. It was a band-aid approach, because we had both drawn a line in the sand. There was clearly a section 7 [*Charter* issue] of rights, disclosure rights and there was clearly a national security interest."[37]

Code testified about what he viewed as the desire by all parties to avoid "…this horrendous Federal Court procedure of going to Ottawa," involving "a document-by-document litigation model"[38] and educating a Federal Court judge about a case on which the trial judge had already spent a year.[39]

7.2.3 Other Experiences with Section 38 of the *Canada Evidence Act*

Although proceedings under section 38 were avoided in the Air India trials, they have been used in other prosecutions. The use of section 38 in the middle of the *R. v. Ribic* trial derailed the prosecution and resulted in a new trial. That prosecution related to the taking of a Canadian soldier hostage in Bosnia. After the Crown had presented its case to the jury over eight days in October, 2002, the accused proposed to call witnesses to give testimony that involved secret information. Although the jury agreed to a postponement while the issue was litigated in the Federal Court under section 38, the trial judge declared a mistrial on January 20, 2003, when it became apparent that an appeal to the Federal Court of Appeal would take place.[40]

---

35 Testimony of Geoffrey Gaul, vol. 88, December 4, 2007, p. 11378.
36 Testimony of Geoffrey Gaul, vol. 88, December 4, 2007, p. 11391.
37 Testimony of Bill Turner, vol. 66, October 25, 2007, pp. 8323-8324.
38 Testimony of Michael Code, vol. 88, December 4, 2007, p. 11385.
39 Testimony of Michael Code, vol. 88, December 4, 2007, p. 11387.
40 See the history leading up to the mistrial as discussed in *R. v. Ribic*, 2004 CanLII 7091 (ON S.C.) at paras. 3-9.

The new trial in *Ribic* ended in a conviction. A key factor in holding that the accused's right to a trial in a reasonable time was not violated was that the accused himself had initiated the section 38 procedure by calling defence witnesses to provide evidence that could involve secret information.[41] In many cases, the Attorney General of Canada will pursue a section 38 order, and in such cases the prosecution might be held responsible for any resulting trial delays.

In 2001, amendments to section 38 of the *Canada Evidence Act*, enacted as part of the *Anti-terrorism Act*, attempted to respond to the delay problem revealed in *Ribic* by requiring all justice system participants, including the accused, to provide early notice to the Attorney General of Canada of an intention to cause the disclosure of sensitive information. The notification requirement, contained in section 38.01, is designed to allow the Attorney General of Canada to take steps to resolve national security confidentiality matters before trial and to reduce the risk that "…proceedings will come to a halt while the matter [is] transferred to the Federal Court for a determination." However, the Government can still invoke the *Canada Evidence Act* provisions during a hearing.[42]

Even if an accused does not give proper early notice under section 38.01, it would be difficult to prevent the accused from calling evidence that may involve secret material or from seeking to cross-examine Crown witnesses in areas that may provoke secrecy claims. The accused's right to make full answer and defence could be at stake. For example, the accused might argue that the need to call or to cross-examine on the evidence became apparent only after the Crown set out its case in court. A terrorism trial could be disrupted, and perhaps aborted, if national security confidentiality issues are raised in the middle of the trial, then litigated in the Federal Court, with the possibility of appeal to the Federal Court of Appeal and further appeal to the Supreme Court of Canada. If the accused was being tried by jury, a mistrial would be quite likely, as in *Ribic*.

Even extensive litigation and appeals of section 38 issues before trial at the insistence of the Attorney General of Canada could delay the trial, raising the possibility that the trial judge will declare a permanent stay of proceedings because of unreasonable delay. As discussed in Chapter IX, terrorism prosecutions already sorely tax the stamina of judges and jurors, even without the addition of section 38 litigation in the Federal Court, possibly followed by appeals.

The *Ribic* case demonstrates how an accused might use the two-court approach – dealing with the trial in one court and with section 38 issues in the Federal Court – to sabotage a terrorism trial by trying to call evidence that leads to section 38 litigation in Federal Court. Once an accused seeks information and the Attorney General of Canada refuses to disclose it, litigation in the Federal Court is inevitable, with appeals likely to the Federal Court of Appeal and the Supreme Court of Canada. This litigation will delay and disrupt the main trial and

---

41 *R. v. Ribic*, 2008 ONCA 790 at paras. 138, 147.

42 Department of Justice Canada, "The *Anti-terrorism Act*, Amendments to the *Canada Evidence Act* (CEA)", online: Department of Justice Canada <http://canada.justice.gc.ca/eng/antiter/sheet-fiche/cea-lpc/cea2-lpc2.html#b> (accessed May 26, 2009).

might result in its collapse. Particularly in a jury trial, it is probable that a mistrial will be declared if there is a serious delay. The Attorney General of Canada has to face the dilemma of agreeing to the disclosure of secret information that should not be disclosed in order to prevent the trial from "going off the rails."

Other proceedings in the *Ribic* prosecution highlighted the complexities, delay and duplication of effort caused by the present two-court approach. *Ribic* involved multiple pre-trial applications before specially-designated Federal Court judges to deal with section 38 issues.[43] Under section 38, the Federal Court can make rulings only about one privilege – national security confidentiality. All other decisions about privileges that may shield information from disclosure, including informer privilege, must be made by the trial judge. Even on national security confidentiality issues, the Federal Court's decision does not end the matter; if the Federal Court makes a non-disclosure order, the trial judge must determine whether to provide a remedy to protect the accused's right to a fair trial.

In *Ribic*, the Federal Court used an innovative approach to reconcile the competing demands for disclosure and secrecy by providing that the two witnesses whose testimony the accused wanted would be asked questions by a security-cleared lawyer. To protect against the inadvertent disclosure of secret information, an edited transcript of the testimony would be disclosed for use at trial.[44] However, the transcript was effectively re-litigated before the trial judge, who had to decide whether the edited transcript could be admitted at trial. The trial judge allowed the edited transcript to be used as evidence, in large part because the transcript related to contextual evidence called by the accused and was not central to the allegations about the accused's conduct.[45] This approach will not easily be duplicated in other cases involving secret information and at its best would simply constitute another "band-aid."

In *Ribic*, a disclosure issue that had been litigated and appealed in the Federal Court[46] was effectively re-litigated before the trial judge. A subsequent appeal by the accused to the Ontario Court of Appeal, on the basis that the trial judge should have stayed proceedings because of limited disclosure and trial delay, was only recently dismissed.[47]

The section 38 procedure requires two different courts to decide similar and closely related issues. Any non-disclosure or partial non-disclosure order made by the Federal Court under section 38 will effectively have to be re-litigated before the trial judge. This re-litigation is required because section 38.14 of the *Canada Evidence Act* requires the trial judge to accept the Federal Court

---

43 See, for example, *Nicholas Ribic and Her Majesty the Queen and Canadian Security Intelligence Service*, 2002 FCT 290 and *Canada (Attorney General) v. Ribic*, 2002 FCT 839, 221 F.T.R. 310.

44 *Ribic v. Canada (Attorney General)*, 2003 FCT 10, 250 F.T.R. 161.

45 *R. v. Ribic*, [2005] O.J. No. 2628 (Sup. Ct.).

46 The Supreme Court refused leave to appeal.

47 *R. v. Ribic*, 2008 ONCA 790. The Ontario Court of Appeal noted that four Federal Court judges had already found that the disclosure process was fair to the accused: see para. 92.

order, but also requires the trial judge to determine if any order is appropriate to protect the accused's right to a fair trial in light of the non-disclosure order. Section 38.14 protects an accused's right to a fair trial. However, it places trial judges in the difficult position of deciding, on incomplete information, whether the right to a fair trial has been compromised by a Federal Court non-disclosure order.

An Ontario Superior Court judge who presided at a 1986 terrorism prosecution involving the predecessor to section 38 made it clear that the two-court procedure placed him in a very difficult position. He indicated that "…the trial judge may well be on the horn of a real dilemma if, in his judgment, inspection is needed."[48] He elaborated:

> Blame must be laid squarely at the feet of Parliament which unwittingly may well have created an impasse in certain cases by resorting to two courts instead of one and assigning tasks to each of them that collide or run at cross-purposes to one another…. There appears to be nothing left to do at trial except to consider the impact of the Federal Court determination on the exigencies of a fair trial…. Parliament could not have intended to give the Federal Court jurisdiction nor, in my opinion, could such jurisdiction be exercised by the Federal Court in such a way as to operate in derogation of the duty imposed on trial judges, as courts of competent jurisdiction, to enforce the rights of the accused in the course of the trial, rights that are now constitutionally entrenched.[49]

The prosecution was allowed to proceed even though no court had examined the CSIS surveillance material about the accused. Such an approach would likely not be acceptable today, given the increased emphasis on the accused's rights to disclosure and to make full answer and defence.

7.2.4 Procedures Equivalent to Section 38 in Other Countries

Canada lags behind other counties, including Australia, the United Kingdom and the United States, in establishing an efficient and fair process to enable judges to determine whether intelligence must be disclosed to ensure a fair trial.

A paper prepared for the Commission by Professor Robert Chesney outlined some of the creative approaches that American trial judges have used to avoid the "disclose or dismiss" dilemma. These approaches included allowing foreign security agents to testify under pseudonyms, presenting depositions by video links and disclosing intelligence material to defence counsel who have undertaken not to share the material with clients.

---

48 *R. v. Kevork, Balian and Gharakhanian* (1986), 27 C.C.C. (3d) 523 at 536 (Ont. H.C.J.).
49 (1986), 27 C.C.C. (3d) 523 at 538, 540 (Ont. H.C.J.).

In Australia, the United Kingdom and the United States, the trial judge is allowed to examine secret information to determine whether its disclosure is necessary for a fair trial. In his study for the Commission, Professor Roach concluded that all three countries "…allow the trial judge to decide questions of non-disclosure. This allows issues of non-disclosure to be integrated with comprehensive pre-trial management of a range of disclosure and other issues. Even more importantly, it allows a trial judge who has seen the secret material to revisit an initial non-disclosure order in light of the evolving issues at the criminal trial…."[50]

Australian legislation enacted in 2004 makes the trial judge responsible for reconciling the competing interests in secrecy and disclosure and for managing issues of national security confidentiality, including requiring defence lawyers to obtain security clearances as a condition of access to secret information. This legislation was enacted after a thorough review of options by the Australian Law Reform Commission.[51]

The European Court of Human Rights held that the ability of the trial judge to see the information and "…to monitor the need for disclosure throughout the trial, assessing the importance of the undisclosed evidence at a stage when new issues were emerging,"[52] was critical to the fairness of the United Kingdom's system of public interest immunity, which has come into play in many UK terrorism prosecutions. The ability of the trial judge to monitor throughout the trial whether disclosure is necessary helps to ensure fair treatment of the accused. This procedure also promotes an efficient trial process by allowing trial judges to make provisional non-disclosure orders, secure in the knowledge that these orders can be revisited as the trial evolves if fairness for the accused requires it. In contrast, the Federal Court often decides disclosure issues under section 38 before the trial has started and before all the issues that will emerge at the trial are known. As well, the trial judge cannot later revise a non-disclosure order under section 38. The trial judge must abide by the order.

The Canadian two-court system has been the subject of international criticism, including in a recent report by the Eminent Jurists Panel on Terrorism, Counter-terrorism and Human Rights:

> In Canada, the trial judges, who must ultimately decide whether to proceed or order a stay of proceedings, are arguably placed in a difficult position of having to assess the potential prejudice of non-disclosure upon the rights of the accused, without seeing the withheld material.[53]

---

50 Roach Paper on Terrorism Prosecutions, p. 286.

51 *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth.); Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, online: Australasian Legal Information Institute <http://www.austlii.edu.au/au/other/alrc/publications/reports/98> (accessed May 28, 2009).

52 *Rowe and Davis v. United Kingdom*, (2000) 30 E.H.R.R. 1 at para. 65. See also *R. v. H; R. v. C*, [2004] UKHL 3 at para. 36, emphasizing that a trial judge's decision not to disclose information because of public interest immunity concerns "…should not be treated as a final, once-and-for-all, answer but as a provisional answer which the court must keep under review."

53 *Assessing Damage, Urging Action*, p. 153.

The report also observed that the United Nations Human Rights Committee expressed concerns that the section 38 procedure might violate the right to a fair trial, a right protected by Article 14 of the *International Covenant on Civil and Political Rights*.[54]

7.2.5 Submissions to the Commission about the Two-Court System under Section 38

The Attorney General of Canada supported the current two-court approach, primarily because the Federal Court "…is comfortable with national security issues, already has the expertise and already has the required secure facilities."[55] The Attorney General warned that taking these matters away from the Federal Court "…could lead to inconsistent applications."[56] The Attorney General also suggested that it was too soon to determine if the two-court process was a failure and stated that the section 38 process was not linked directly to the trial process.[57] The Attorney General also submitted that the person holding that office would continue to weigh the competing interests for and against disclosure after the Federal Court had ruled on disclosure.[58]

Other witnesses, parties and intervenors before the Commission were almost unanimous in concluding that the current two-court system was inadequate and could cause problems.[59] George Dolhai, of the Public Prosecution Service of Canada, noted that this approach was not used in the United States, Britain or Australia.[60] Jack Hooper, an experienced former CSIS official, stated that the present system was not "…a particularly useful bifurcation…. I think it has an alienating effect on provincial Crown and provincial judges who sit in the weighty position of having to rule on evidence put before the court."[61] Luc Portelance of CSIS testified that the "…bifurcated system is complex, complicated and probably contributes to a loss of momentum in the case."[62] Former RCMP Commissioner Giuliano Zaccardelli stated that legislative change was required "…because using two courts, two judges, simply is not effective and efficient and it has to change. I see no reason why we cannot have one judge who, wherever the case is being heard, for that judge – to say that a judge could look at everything other than this, it's almost insulting to the judge as far as I'm concerned."[63]

---

54 *Assessing Damage, Urging Action*, p. 153.
55 Final Submissions of the Attorney General of Canada, Vol. III, February 29, 2008, para. 92 [Final Submissions of the Attorney General of Canada].
56 Final Submissions of the Attorney General of Canada, Vol. III, para. 93.
57 Final Submissions of the Attorney General of Canada, Vol. III, para. 90.
58 Final Submissions of the Attorney General of Canada, Vol. III, para. 110.
59 Testimony of John Norris, vol. 86, November 30, 2007, pp. 11127-11129; Testimony of Gérard Normand, vol. 86, November 30, 2007, p. 11129; Testimony of Kent Roach, vol. 86, November 30, 2007, pp. 11131-11132.
60 Testimony of George Dolhai, vol. 86, November 30, 2007, p. 11136.
61 Testimony of Jack Hooper, vol. 50, September 21, 2007, p. 6247.
62 Testimony of Luc Portelance, vol. 88, December 4, 2007, p. 11507.
63 Testimony of Giuliano Zaccardelli, vol. 86, November 30, 2007, p. 11071.

The Criminal Lawyers' Association also addressed the section 38 process:

> **The section 38 process is unworkable.** The need to go to a different court in a different location, before or during the trial slows down the proceedings. The Federal Court is at a disadvantage in not having the full context of the evidence and providing that context is time-consuming for the parties. The trial judge is in the best position to make the necessary determinations under section 38.
>
> **Appellate review by the Federal Court of Appeal also creates the same issues** - multiplication of interlocutory proceedings and determinations made without full context.
>
> **The lack of criminal law experience of Federal Court judges** is also an issue.
>
> **Senior superior court judges who preside over terrorism cases should have the power to deal with section 38 claims** (either by amending section 38 or by designating the judges as *ex officio* members of the Federal Court and allowing the proceedings to take place in locations other than Ottawa.)[64]

The Air India Victims' Families Association also supported moving away from the two-court approach. To preserve the important role of trial by jury, the Association suggested that the court hearing section 38 disclosure issues should be the provincial superior court.[65]

After the Commission hearings ended, the Hon. Patrick LeSage and Michael Code produced a report on long and complex criminal cases. They recommended that federal, provincial and territorial ministers of justice should consider modifying the section 38 procedure "…in order to eliminate the delays caused in major terrorism prosecutions by the bifurcation of the case and by interlocutory appeals."[66] Drawing on their many years of experience with the criminal justice system, LeSage and Code explained that almost every terrorism prosecution will involve attempts to obtain disclosure and to call evidence from CSIS:

---

64 From Yolanda's summary but can't find in submissions

65 AIVFA Final Written Submission, pp.131, 168.

66 Patrick Lesage and Michael Code, *Report of the Review of Large and Complex Criminal Case Procedures* (November 2008), p. 93, online: Ontario Ministry of the Attorney General <http://www.attorneygeneral.jus.gov.on.ca/english/about/pubs/lesage_code/lesage_code_report_en.pdf> (accessed December 5, 2008) [Lesage and Code Report on Large and Complex Criminal Case Procedures].

> As a result of this intersection between CSIS and RCMP investigations in the context of terrorism offences, national security privilege claims pursuant to s. 38 of the *Evidence Act* are now a common feature of these cases. These privilege claims raise very difficult case management problems. … Bifurcation of criminal trials and interlocutory appeals in criminal proceedings have both been regarded as an anathema for a very long time because they fragment and delay the criminal trial process.[67]

LeSage and Code contemplated that experienced superior court trial judges could decide section 38 issues as part of the trial process and that their decisions would be subject to ordinary appeal procedures, but only after the completion of the trial.

7.3 Is the Two-Court Approach Sustainable

The present two-court system used in deciding section 38 applications is out of step with systems in other democracies. The two-court structure has demonstrated unequivocally that it is a failure.

It is not likely that the two-court system can be saved. One unworkable suggestion was to facilitate communication between the Federal Court judge and the trial judge by amending section 38.05. However, the trial judge would not be permitted to examine the sensitive information in the first place.

Section 38.14 recognizes that the trial judge has a duty to protect the accused's right to a fair trial. The trial judge also has remedial powers under section 24(1) of the *Charter*.[68] However, under the current system, the trial judge does not have the information that is required to craft the appropriate remedy under section 38.14 or under section 24(1) of the *Charter*.

The trial judge can apply a range of remedies in response to a non-disclosure order, including a stay of proceedings. However, the trial judge has no authority to impose what will often be the most appropriate remedy – revision of the Federal Court's non-disclosure order in light of changed circumstances.

The problems of the current two-court system are real and serious. A trial judge might permanently halt a terrorism prosecution under section 38.14 as a result of a non-disclosure order made by the Federal Court. As Geoffrey O'Brian, Director General of Operations at CSIS, testified, "…the issue is not necessarily, can you protect that information? The issue, it seems to me, is: having protected that information, is it fatal to the prosecution? And that's the issue I think that perhaps is the tough one."[69]

---

67 Lesage and Code Report on Large and Complex Criminal Case Procedures, pp. 91-92.
68 *R. v. Ribic*, 2008 ONCA 790 at para. 113.
69 Testimony of Geoffrey O'Brian, vol. 17, March 6, 2007, p. 1582.

Another harm of the current two-court system is that a trial judge who has not seen the secret intelligence that is the subject of a Federal Court order might wrongly conclude that the accused does not need that secret intelligence to make full answer and defence. The result would be an unfair trial.

If a trial judge were allowed to examine the secret information that was the subject of an earlier non-disclosure order, the judge might determine that the information would not be helpful to the accused and that, as a result, the non-disclosure order did not make the trial less fair. If the judge determined that the undisclosed intelligence might be of some use to the accused, the judge could revise an initial non-disclosure order to allow parts of the intelligence to be disclosed to the accused or to require the prosecution to make admissions to compensate for the non-disclosure.

The Attorney General of Canada has submitted that the rationale for the two-court system is the expertise that has been developed by specially designated judges of the Federal Court in deciding matters of national security confidentiality. The need for special expertise to make decisions about national security confidentiality has, in the view of the Commission, been exaggerated.

The first step in the section 38 process as applied to criminal prosecutions is to determine whether the material in dispute is "relevant" in accordance with *Stinchcombe*. This is a matter traditionally decided by trial judges in criminal cases.

If the trial judge determines that the information is relevant, a second step is necessary to determine if disclosing the information would cause harm to international relations, national security or national defence. This is a matter currently within the jurisdiction of specially designated Federal Court judges. The practice at this stage is to accept the Attorney General's claim of injury so long as it is reasonable.[70] If trial judges were allowed to address this issue, they, like Federal Court judges, could be assisted by the *ex parte* submissions of the Attorney General of Canada about the risks flowing from disclosing the information in question.

Finally, the critical step under section 38 is to reconcile the competing demands for disclosure and non-disclosure. The Federal Court of Appeal has expressed a preference that this process be governed by the innocence-at-stake exception,[71] a test well within the competence of trial judges, who face it frequently.

In addition, section 38.06 encourages judges to devise creative solutions, using partial redactions and admissions of fact. Trial judges would be in the best position to devise such tailored remedies on the basis of all the facts in the case before them. As discussed earlier, if Federal Court judges devise the same types of tailored remedies, they will effectively have to be re-litigated before the trial judge, who retains ultimate control over how evidence is presented

70 *Canada (Attorney General) v. Ribic*, 2003 FCA 246, 185 C.C.C (3d) 129 at paras. 18-19.
71 *Canada (Attorney General) v. Ribic*, 2003 FCA 246, 185 C.C.C (3d) 129 at para. 27.

at trial. Allowing trial judges to make disclosure decisions would avoid this re-litigation.

It is incorrect to suggest, as the Attorney General of Canada did in his Final Submissions to the Commission, that section 38 proceedings are not linked directly to the trial process. Section 38 procedures are used to resist production and disclosure of intelligence to the accused. In principle, section 38 involves an assertion of a privilege that limits the amount of material that the accused and the trial court can have at their disposal at trial. In that sense, section 38 privilege claims are similar to other privilege claims advanced in a trial proceeding. Moreover, under section 38.14, the trial judge plays a critical role in deciding whether a remedy for the accused is necessary to compensate for a Federal Court order for non-disclosure or modified disclosure. The trial judge is left with the ultimate responsibility of dealing with the consequences of any decision by the Federal Court about disclosure. At the cost of repetition, the section 38 process affects both the efficiency and the fairness of terrorism prosecutions and is therefore clearly and directly linked to the trial process.

The Attorney General of Canada argued that allowing trial judges to make section 38 determinations could lead to inconsistent applications of the law. This does not seem to be a problem in other countries that allow trial judges to decide disclosure issues similar to those addressed by section 38. Canadian trial judges, by virtue of their oaths of office, would follow authority in the existing jurisprudence, as it has been developed by the Federal Court and by the Federal Court of Appeal. The *Criminal Code*[72] provides a good example of how federal legislation is applied across the country by superior and provincial courts with little inconsistency among jurisdictions. In any event, the Supreme Court of Canada can resolve any inconsistencies that may arise among courts in interpreting section 38.

The Supreme Court has yet to interpret section 38. This is in part because section 38 issues have often arisen in appeals that are launched before or, as in *Ribic*, during criminal trials. In all these cases, the Court has refused leave to appeal. Granting leave to appeal would have caused even more delay in an already strained trial process. The Court may be better placed to offer guidance about the interpretation of section 38 if this is raised, as with other issues about disclosure and privilege, on appeal after a trial is completed.

In summary, there are serious and irremediable disadvantages to the current two-court system for resolving issues of national security confidentiality. The Federal Court does not have full information about the trial, while the criminal trial judge does not have full information about the secret information that is subject to a non-disclosure order. Section 38 litigation, as it is currently, delays and disrupts terrorism prosecutions, while leaving the trial judge to decide what, if any, remedy is necessary to compensate the accused for the lack of disclosure. The trial judge may have to rely on blunt remedies, including a stay

72 R.S.C. 1985, c. C-46.

of proceedings that will permanently end the prosecution. The trial judge is not able to revise the non-disclosure order, even though this power is considered to be critical in other countries that deal with the same issues of reconciling competing interests in disclosure and secrecy.

Canada's allies trust trial judges to make decisions about the disclosure of secret information, including information provided by allies. In addition, trial judges regularly deal with informer privilege issues where an inadvertent leak of information could result in an informer's death.

7.4 Which Court is Best Suited to Conduct Terrorism Trials and Decide Issues of National Security Confidentiality

The Commission has concluded that a one-court approach to deciding section 38 issues is necessary. The next step is to decide which court – the regular criminal courts or the Federal Court – is best suited to conduct terrorism trials and to make section 38 determinations. The Commission recommends that it should be the regular criminal courts. The Federal Court would retain jurisdiction, as would the superior courts, to hear section 38 applications, but the Federal Court would cease its involvement as soon as the trial begins.

There has been some interest in the United States in creating a national security court to try terrorism cases. However, the US, the United Kingdom and Australia have all had significant successes with the regular criminal courts conducting terrorism prosecutions that involve secret information. The Canadian Bar Association, in its submissions, strongly argued against a special court system for terrorism offences.[73] Both before and after 9/11, attempts in other countries to have an adjudicative body dedicated only to terrorism trials have not been particularly successful.[74]

In his testimony, Jack Hooper expressed a preference for the Federal Court to conduct terrorism trials because of the Court's expertise in national security matters.[75] However, Bruce MacFarlane noted in his paper for the Commission that there is great value in having terrorism trials tried in the regular criminal courts.[76]

The Federal Court is a statutory court with many statutory responsibilities of importance to Canada. When the Federal Court evolved from the Exchequer Court in 1976, it was never intended that the new Court would have criminal jurisdiction. Although terrorism trials involve secret information, including secret information obtained from other countries, they remain criminal trials,

73 Canadian Bar Association, Submission to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, April 2007, p. 36 [Canadian Bar Association Submission].

74 See the history of such attempts discussed in Bruce MacFarlane, "Structural Aspects of Terrorist Mega-Trials: A Comparative Analysis" in Vol. 3 of Research Studies: Terrorism Prosecutions [MacFarlane Paper on Terrorist Mega-Trials].

75 Testimony of Jack Hooper, vol. 50, September 21, 2007, p. 6248.

76 MacFarlane Paper on Terrorist Mega-Trials.

raising a host of procedural, evidential and substantive issues which are best addressed by experienced criminal law judges.

Assigning terrorism trials to the Federal Court might also produce constitutional difficulties. Roach noted in his paper for the Commission that assigning terrorism trials to the Federal Court might be challenged as violating the inherent and constitutionally guaranteed jurisdiction of the provincial superior courts over what, as in the Air India prosecutions, may essentially be murder trials.[77] He suggested that "…it is better to build national security expertise into the existing criminal trial courts than to attempt to give a court with national security expertise but no criminal trial experience the difficult task of hearing terrorism trials."[78]

The preferred solution would be to adopt the practice used in the United States, the United Kingdom and Australia, which would allow superior court trial judges to reconcile the competing demands of disclosure and secrecy. Like some other witnesses, George Dolhai cautioned, but not persuasively, that it was too soon to change section 38. Still, he agreed that not only the Americans, but also the British and, most recently, the Australians "…have all seen fit to assign these complex secrecy issues – to assign them to trial judges as just another issue that has to be continuously managed before and during trial."[79]

One concern was that trial courts would not have the facilities to store and protect secret information,[80] a concern that hardly warrants comment, since superior courts across the country are already able to offer such protection. As John Norris, an experienced defence counsel, testified, the trial courts already handle highly sensitive material that could identify informers and that involve organized crime.[81]

Claims by the Attorney General of Canada and by RCMP Commissioner William Elliott[82] that provincial superior court trial judges lack sufficient expertise in dealing with secret information have no merit. To repeat, much of the section 38 decision-making process turns on matters such as relevance, the right to make full answer and defence and "innocence-at–stake." Experienced criminal trial judges have the expertise to deal with all these issues. As is now done for Federal Court judges, criminal trial judges, under a reformed section 38 hearing process, would receive confidential submissions by the Attorney General of Canada about the harms that disclosing secret information may cause to national security, national defence or international relations.

---

77 Roach Paper on Terrorism Prosecutions, pp. 311-312.
78 Roach Paper on Terrorism Prosecutions, p. 313.
79 Testimony of George Dolhai, vol. 86, November 30, 2007, p. 11136. See also Testimony of Andrew Ellis, vol. 82, November 23, 2007, pp. 10576-10577.
80 Testimony of Gérard Normand, vol. 86, November 30, 2007, pp. 11134-11135.
81 Testimony of John Norris, vol. 86, November 30, 2007, p. 11136.
82 Testimony of William Elliott, vol. 90, December 6, 2007, p. 11811.

As is the normal practice, the chief justice of each provincial superior court would select the judges to hear cases involving section 38 applications. Appointing experienced trial judges to hear section 38 matters early in the trial process would promote efficient case management. As Chapter IX suggests, efficient case management is essential if complex terrorism cases are to proceed efficiently and fairly to a verdict. Someone must be in charge of the complex criminal trial process. This includes taking responsibility for decisions that reconcile the competing demands of secrecy and disclosure, along with those involving multiple pre-trial motions and voluminous disclosure of other materials. As in other countries, the best person to take the lead and to ensure that terrorism prosecutions can be brought to verdict efficiently and fairly is the trial judge.

Recommendation 19:

The present two-court approach to resolving claims of national security confidentiality under section 38 of the *Canada Evidence Act* should be abandoned for criminal cases. Section 38 should be amended to allow the trial court where terrorism charges are tried to make decisions about national security confidentiality. Section 38 should be amended to include the criminal trial court in the definition of "judge" for the purposes of dealing with a section 38 application that is made during a criminal prosecution.

7.5 Appeals before the Completion of Terrorism Trials

The criminal law normally does not allow the accused or the Crown to appeal pre-trial and mid-trial rulings until after the completion of a trial. As an example, the accused cannot appeal a trial judge's decision that a confession was voluntary or constitutionally obtained until the completion of the trial. The same limitations apply to the Crown. The rationale for this traditional policy against interlocutory appeals, or appeals before the completion of trials, is the compelling public interest in completing trials in an efficient manner.[83] There is arguably no public interest in allowing appeals mid-way in the trial. With jury trials, interlocutory appeals might require a completely new trial and a new jury. Even this would not end the possibility of further appeals under section 38. In addition, the issues argued under section 38 on an appeal taken before the end of the trial may have been resolved by the time the trial ends. An appeal on those issues may turn out to have been unnecessary.

Sections 37.1 and 38.09 of the *Canada Evidence Act* allow appeals, both by the accused and by the Attorney General of Canada, from a decision made by a trial judge under section 37 or by a Federal Court judge under section 38. Sections

---

83 "The effective and efficient operation of our criminal justice system is not served by interlocutory challenges to rulings made during the process or by applications for rulings concerning issues which it is anticipated will arise at some point in the process. A similar policy is evident in those cases which hold that interlocutory appeals are not available in criminal matters.": *R. v. Duvivier*, (1991) 64 C.C.C. (3d) 20 at 24 (Ont. C.A.).

37.1 and 38.09 allow appeals about the disclosure matters dealt with in these sections to proceed before a criminal trial starts. They also authorize the appeal of such issues if they arise during a trial.

In the two criminal prosecutions since 2001 that have involved section 38, the Federal Court of Appeal heard appeals before the criminal trial was completed.[84] The potential for multiple section 38 applications in a terrorism prosecution means the potential for multiple appeals in turn. These appeals unquestionably delay the criminal trial, and still further delay will occur if the losing party seeks leave to appeal to the Supreme Court of Canada and, if successful, has a hearing before the Court.

The Attorney General of Canada has defended the value of interlocutory appeals under section 38.09, arguing that they "…maintain the public interest in a trial proceeding to verdict in a timely manner and, at the same time, may preclude recourse to the use of a prohibition certificate by the Attorney General of Canada under section 38.13 of the [*Canada Evidence Act*]."[85] The concern seems to be that a decision ordering disclosure, if it could not be appealed immediately, might force the Crown to abandon the prosecution if it did not want to disclose the information. These arguments, however, ignore the authority of the Attorney General of Canada to act under section 38.13 where he concludes that disclosure is contrary to the public interest.

The submission of the Criminal Lawyers' Association stated that interlocutory appeals "…inevitably [generate]…excessive delays in the criminal proceedings, sometimes to the extent where the *Charter* right to a speedy trial is engaged." Code stated in his testimony before the Commission that, "The interlocutory appeals are anathema…. [T]hey've never been allowed in the criminal process and the fact that section 38 currently provides for interlocutory appeals, in my opinion, is flatly wrong."[86] A subsequent report by the Hon. Patrick Lesage and Code recommended that these interlocutory appeals be eliminated.[87]

The traditional practice of not hearing appeals before the completion of criminal trials is of long standing and remains sound. Requiring appeals of section 38 matters to await the completion of the trial would allow the appeal court to make its decision on the basis of the complete record.

If appeals are not permitted until after the completion of the trial, the full record will then be available to the court to determine whether the accused's rights were adversely affected by non-disclosure orders made under sections 37 and 38 or by a prohibition certificate issued by the Attorney General of Canada after an order to disclose.

---

84 See *Canada (Attorney General) v. Ribic*, 2003 FCA 246, 185 C.C.C. (3d) 129; *Canada (Attorney General) v. Khawaja*, 2007 FCA 342, 228 C.C.C. (3d) 1; *Canada (Attorney General) v. Khawaja*, 2007 FCA. 388, 289 D.L.R. (4th) 260.

85 Final Submissions of the Attorney General of Canada, Vol. III, para. 59.

86 Testimony of Michael Code, vol. 88, December 4, 2007, p. 11388.

87 Lesage and Code Report on Large and Complex Criminal Case Procedures, p. 93.

The Federal Court of Appeal might order disclosure of information that the Federal Court originally ordered not be disclosed. The Attorney General of Canada can acquiesce, or can instead prevent the disclosure of the information. To prevent disclosure, the Attorney General can issue a non-disclosure certificate under section 38.13. He can also stay a prosecution or assert his fiat under the *Security Offences Act*[88] and then stay the prosecution.

Section 38.09 authorizes the Federal Court of Appeal to hear appeals of section 38 matters that arise in criminal trials. The Federal Court of Appeal should no longer hear such appeals. Instead, the *Canada Evidence Act* should be amended to authorize only provincial courts of appeal to hear the appeals, and the appeals should be heard only at the conclusion of the trial. Section 37.1 already authorizes provincial courts of appeal to hear appeals where an application for public interest immunity has been made in a criminal trial. Allowing appeals of section 38 matters to be heard by the same courts would avoid fragmenting the appeal process. Provincial courts of appeal would then be able to hear appeals about all the legal issues arising from a terrorism trial, including those relating to section 38. This proposal to expand the jurisdiction of provincial courts of appeal would complement the expanded jurisdiction of trial judges, proposed earlier, to decide section 38 issues in terrorism trials.

Recommendation 20:

In terrorism prosecutions, there should be no interim appeals or reviews of section 37 or 38 disclosure matters. Appeals of rulings under sections 37 or 38 should not be permitted until after a verdict has been reached. Appeals should be heard by provincial courts of appeal in accordance with the appeal provisions contained in the *Criminal Code*. If not already in place, arrangements should be made to ensure adequate protection of secret information that provincial courts of appeal may receive. Sections 37.1, 38.08 and 38.09 of the *Canada Evidence Act* should be amended or repealed accordingly.

7.6 Possible Use of Special Advocates in Section 38 Proceedings

Special advocates are lawyers who have received high-level security clearances and can therefore have access to secret material. They can represent the interests of individuals in proceedings where the individuals and their lawyers would be denied access to the secret material. Chapter IV discusses the role of special advocates in proceedings that challenge the legality and constitutionality of warrants.

At present, there is a statutory regime for special advocates for proceedings under the *Immigration and Refugee Protection Act*.[89] This has led to the creation

88 R.S.C. 1985, c. S-7.

89 S.C. 2001, c. 27. The regime for special advocates was introduced by *An Act to amend the Immigration and Refugee Protection Act (certificate and special advocate) and to make a consequential amendment to another Act*, S.C. 2008, c. 3.

of a cadre of security-cleared lawyers with experience in matters involving national security confidentiality.

Special advocates should have a similar role in proceedings under section 38 of the *Canada Evidence Act*. Section 38.11(2) provides that the Attorney General of Canada may make *ex parte* representations to a judge. The *ex parte* nature of the hearing allows the Attorney General to describe the secret information that may become the subject of a non-disclosure order and to provide confidential details about the harms that disclosure might cause.

Although permitted in some situations, typically during an application for a search warrant, legal proceedings with only one side present before the judge are not the norm. They depart from basic standards of adjudicative fairness. They place judges, accustomed to adversarial argument, in a very difficult position. The interests of the accused and of the judge who decides the matter will be better served if there is an opportunity, through special advocates, for adversarial argument about critical matters – such as whether secret information would be helpful to the accused and whether the claims by the Attorney General about the possible harms of disclosure are valid.

In addition, special advocates could assist in finding ways to reconcile competing interests in disclosure and secrecy – for instance, through partial disclosure of the material.

The Federal Court has appointed security-cleared *amici curiae* to assist it in recent proceedings under section 38 of the *Canada Evidence Act*.[90] The availability to the Court of *amici curiae* has been cited as one reason why section 38 has been found to be consistent with the *Charter*, despite allowing the Attorney General to make submissions to the judge without the accused present.[91]

The Attorney General of Canada, in its Final Submissions, recognized the "inherent discretion" of the Federal Court to appoint an *amicus curiae* as a legal expert to assist the court on national security matters. The Attorney General, however, distinguished the *amicus curiae* from the special advocate who would protect the interests of the accused.[92] The Attorney General, unhelpfully and without persuasive submissions, noted the Government's position that further study was required before special advocates could be used in section 38 proceedings.[93]

There has already been extensive study and extensive support for using special advocates in section 38 proceedings. The House of Commons and

---

90 *Khadr v. Canada (Attorney General)*, 2008 FC 46, 54 C.R. (6th) 76; *Canada (Attorney General) v. Khawaja*, 2008 FC 560; *Khadr v. Canada (Attorney General)*, 2008 FC 807.

91 *Canada (Attorney General) v. Khawaja*, 2007 FC 463, 280 D.L.R. (4th) 32 at para. 59, affirmed without reference to special advocates, *Canada (Attorney General) v. Khawaja*, 2007 FCA 388, 289 D.L.R. (4th) 260.

92 Final Submissions of the Attorney General of Canada, Vol. III, para. 51.

93 Final Submissions of the Attorney General of Canada, Vol. III, para. 53.

Senate committees that reviewed the operation of the *Anti-terrorism Act* both recommended that provision be made for special advocates to provide adversarial challenges to Government claims under section 38 about the need for secrecy.[94] The Federation of Law Societies of Canada, the Canadian Bar Association and the Criminal Lawyers' Association all supported the use of special advocates in section 38 proceedings.[95] The Federation of Law Societies stressed that the accused's *Charter* rights to disclosure and to make full answer and defence were at stake in section 38 proceedings, and that Canada's justice system was based on an adversarial system.[96] It cited the statement by Justice Hugessen of the Federal Court at a recent Montreal conference: "[W]e do not like this process of having to sit alone hearing only one party, and looking at the materials produced by only one party…."[97]

Section 38 proceedings are important matters that implicate the accused's rights to disclosure and to make full answer and defence. The judge who is given the difficult task of reconciling competing interests in secrecy and disclosure should be assisted by the fully-informed adversarial arguments that special advocates can offer. Full adversarial argument is particularly necessary because of the tendency of the Attorney General of Canada to overstate the need for secrecy. The accused themselves, through their own counsel, should be permitted to make submissions in section 38 proceedings, although they will be at a considerable disadvantage because they will not have seen the secret material or heard the Attorney General's *ex parte* arguments about the dangers of disclosing the secret material.

The special advocates appointed to deal with *Immigration and Refugee Protection Act* matters could just as well be used for section 38 proceedings. They already have security clearances and could be available without delay.

Recommendation 21:

Security-cleared special advocates should be permitted to protect the accused's interests during section 38 applications, in the same manner as they are used under the *Immigration and Refugee Protection Act*. Either the accused or the presiding judge should be permitted to request the appointment of a special advocate.

---

94 House of Commons Canada, Final Report of the Standing Committee on Public Safety and National Security, Subcommittee on the Review of the *Anti-terrorism Act*, *Rights, Limits, Security: A Comprehensive Review of the Anti-terrorism Act and Related Issues*, March 2007, p. 81, online: Parliament of Canada <http://www2.parl.gc.ca/content/hoc/Committee/391/SECU/Reports/RP2798914/sterrp07/sterrp07-e.pdf> (accessed July 30, 2009); The Senate of Canada, *Fundamental Justice In Extraordinary Times: Main Report of the Special Senate Committee on the Anti-terrorism Act*, February 2007, p. 42, online: Parliament of Canada <http://www.parl.gc.ca/39/1/parlbus/commbus/senate/Com-e/anti-e/rep-e/rep02feb07-e.pdf> (accessed July 30, 2009).

95 Submissions of the Federation of Law Societies of Canada, January 31, 2008, p. 2 [Submissions of the Federation of Law Societies of Canada]; Canadian Bar Association Submission, p. 38; Submissions of the Criminal Lawyers' Association, February 2008, pp. 40-41.

96 Submissions of the Federation of Law Societies of Canada, pp. 7-8.

97 Submissions of the Federation of Law Societies of Canada, p. 8.

7.7 The Problems Created by Overstating the Need for Secrecy

The excessive claims about the need for secrecy made by the Attorney General of Canada, during both this inquiry and during the inquiry into the activities of Canadian officials in relation to Maher Arar, were discussed in Volume One. In several recent cases, judges concluded that the Attorney General of Canada failed to demonstrate that the disclosure of information for which a section 38 non-disclosure order was being sought would harm international relations, national security or national defence.[98] Such findings should not be ignored, given the deference shown by the courts to claims made by the Attorney General about the need for secrecy and their willingness to overturn the claims only if they are unreasonable.[99]

Canada is a net importer of intelligence and must protect both its secrets and those of its allies. However, this does not excuse overstating the need for secrecy. An obsessive and risk-averse "culture of secrecy" is a product of Cold War assumptions about the overriding importance of secrecy. It is not appropriate in an age in which terrorism is the primary threat to national security and when information must be shared more extensively than during the Cold War era in order to prevent and prosecute terrorism.

Canada's allies are also being forced to rethink their approaches to secrecy because of the threat of terrorism. The need for disclosure of "secret" information has increased. The need in some situations for intelligence to be used as evidence in terrorism prosecutions has changed the approach of intelligence agencies to collecting information and sharing it with police agencies.

Exaggerating the need for secrecy is not simply something that makes it more difficult for commissions of inquiry such as this one to conduct their work: such exaggeration can threaten public safety. It prevents the sharing among, and within, governments of information that is necessary to prevent terrorism. Unnecessary emphasis on the need for secrecy encourages a narrow, "silo"-based, approach to national security, leading to the results that have been witnessed in terrorist attacks.

Overstating the need for secrecy can also impair the viability of terrorism prosecutions by leading to otherwise unnecessary section 38 applications for non-disclosure orders. Roach stated that overly broad secrecy claims "…can delay and fragment terrorism trials through the use of the s. 38 procedure. They can create the impression that the accused is being denied access to much vital information and this could even result in a trial judge concluding under s. 38.14 that a remedy was required to protect the accused's right to a fair trial."[100]

---

98 *Canada (Attorney General) v. Canada (Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar)*, 2007 FC 766, 316 F.T.R. 279; *Canada (Attorney General) v. Khawaja*, 2007 FC 490, 219 C.C.C. (3d) 305.

99 *Canada (Attorney General) v. Ribic*, 2003 FCA 246, 185 C.C.C. (3d) 129 at paras. 18-19.

100 Roach Paper on Terrorism Prosecutions, p. 195.

It is particularly disappointing that a pattern of overstating the need for secrecy has emerged in Canada after 9/11, when Canada's allies have placed increased emphasis on sharing information about terrorism. Constantly seeking to protect secrecy suggests that the Attorney General may not fully appreciate the current need to share security intelligence and to conduct terrorism prosecutions that involve that intelligence. Even if Canada's status as a net importer of intelligence may require it to be very diligent in protecting the information it receives from foreign agencies, this is not an excuse for overstating the need for secrecy.

Overstating the need for secrecy may allow some officials to avoid criticism, embarrassment and difficult decisions, but it carries a heavy cost. In his 2006 report, Commissioner O'Connor warned that excessive claims for secrecy would endanger the fairness of some proceedings and that they would damage the Government's credibility when it claimed secrecy in the future:

> [O]verclaiming exacerbates the transparency and procedural fairness problems that inevitably accompany any proceeding that can not be fully open because of NSC [national security confidentiality] concerns. It also promotes public suspicion and cynicism about legitimate claims by the Government of national security confidentiality…. I am raising the issue of the Government's overly broad NSC claims in the hope that the experience in this inquiry may provide some guidance for other proceedings. In legal and administrative proceedings where the Government makes NSC claims over some information, the single most important factor in trying to ensure public accountability and fairness is for the Government to limit, from the outset, the breadth of those claims to what is truly necessary. Litigating questionable NSC claims is in nobody's interest. Although government agencies may be tempted to make NSC claims to shield certain information from public scrutiny and avoid potential embarrassment, that temptation should always be resisted.[101]

Unfortunately, Commissioner O'Connor's warnings about the dangers of overstating the need for secrecy have not been heeded. This is confirmed by the experience of this Commission, with the Attorney General of Canada overstating the need for secrecy. As well, several Federal Court decisions have found that the Attorney General brought section 38 claims about irrelevant information and where the Attorney General could not establish that disclosure of the

---

101 Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (Ottawa: Public Works and Government Services Canada, 2006), pp. 302, 304 [*Report of the Events Relating to Maher Arar: Analysis and Recommendations*].

information would harm national security, national defence or international relations.[102]

The practice of overstating the need for secrecy is relevant to the policy mandate of this Commission because the practice can prevent the sharing of information that is necessary for effective cooperation between departments and agencies in terrorism investigations and because it brings added, and unnecessary, complexity to terrorism prosecutions. Changes in practice and in legislation are required.

7.7.1 Towards a More Disciplined and Harm-based Approach to Claims of Secrecy

One cause of the practice of overstating the need for secrecy is the use of broad terms in section 38 of the *Canada Evidence Act* to identify the scope of the secret information involved and the harms that disclosure can cause. The duty to notify the Attorney General of Canada about the possibility of disclosure applies to two broad categories of information:

- "potentially injurious information," defined as "…information of atype that, if it were disclosed to the public, could injure international relations or national defence or national security;" and
- "sensitive information," defined as "…information relating to international relations or national defence or national security that is in the possession of the Government of Canada, whether originating from inside Canada or outside Canada, and is of a type that the Government of Canada is taking measures to safeguard."

The definition of "potentially injurious information" is sufficiently circumscribed. However, the definition of "sensitive information" is too broad. The definition of sensitive information can apply to information that Canada is taking measures to safeguard – for example, information relating to national security – whether or not it is reasonable to safeguard that information. The definition can apply to information that, even if disclosed, could not cause harm.

Section 38 is designed to prevent harm to international relations, national defence or national security that can be caused by the disclosure of information. These are extremely broad and vague terms. Courts have attempted to define these terms. Justice Noël of the Federal Court has examined issues relating to definitions at length, noting that "national security" means "…at minimum the preservation of the Canadian way of life, including the safeguarding of the security of persons, institutions and freedoms in Canada."[103] He described

---

102 *Canada (Attorney General) v. Canada (Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar)*, 2007 FC 766, 316 F.T.R. 279; *Canada (Attorney General) v. Khawaja*, 2007 FC 490, 219 C.C.C. (3d) 305.

103 *Canada (Attorney General) v. Canada (Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar)*, 2007 FC 766, 316 F.T.R. 279 at para. 68.

"national defence" as including "…all measures taken by a nation to protect itself against its enemies" and "a nation's military establishment," while "information injurious to international relations" was referred to as "…information that if disclosed would be injurious to Canada's relationship with foreign nations."[104] These attempts to define the vague statutory terms have tended to make the terms even broader and more vague. In short, there are limits to what can be achieved through definitions of inherently broad and vague terms.

It would be helpful for Parliament to put some flesh on the bare bones of section 38 and provide some concrete examples of particular harms to international relations, national defence and national security. Jim Judd, Director of CSIS at the time of his testimony, stated that section 38 was used mainly to protect secret methods of investigation, information received from foreign authorities that was subject to caveats, and risks to sources and CSIS employees.[105]

In its Final Submissions, the Attorney General of Canada suggested that "…[i]n practical terms, intelligence information relating to international relations, national defence or national security information may include information that reveals or tends to reveal: the identity of a confidential source of information; targets of an investigation; technical sources of information; methods of operation/investigative techniques; the identity of covert employees; telecommunications and cipher systems (cryptology); confidential relationship with a foreign government/agency."[106] This list is long, but it is more helpful than vague references to national security, national defence and international relations.

There is much to be said for a practical approach that focuses on concrete harms caused by the disclosure of secret information rather than on the vague generalities of harm to national security, national defence or international relations. Even if the list of concrete manifestations of harms was not exhaustive, it would help to guide and to limit the Attorney General of Canada's claims of national security confidentiality. It would also help to define the scope of the range of security classifications within government generally. Finally, it would assist judges to make decisions under section 38 of the *Canada Evidence Act*.

As is the case with the *CSIS Act*[107], there is a need to reconsider when to claim secrecy, in order to accommodate today's threat environment where terrorism, not foreign espionage, is the main threat. As the description of the Air India investigation in this report makes clear, obsession with the need for secrecy prevented the exchange of information between agencies in circumstances highly relevant to the destruction of Flight 182.

---

104 2007 FC 766, 316 F.T.R. 279 at paras. 61-62.
105 Testimony of Jim Judd, vol. 90, December 6, 2007, pp. 11861-11862.
106 Final Submissions of the Attorney General of Canada, Vol. III, para. 44.
107 R.S.C. 1985, c. C-23.

7.8 Evolving National Security Confidentiality Jurisprudence

The jurisprudence about national security confidentiality is starting to acknowledge the need for increased exchanges of information to prevent and prosecute terrorism. The "third party rule" prohibits an agency that receives confidential information from a third party from disclosing the information without the third party's consent. This rule evolved to recognize the importance of requesting the third party to amend restrictions that it placed on disclosure.

Canada must respect the caveats that its allies place on disclosing secret information that they share with Canada. In his report, Commissioner O'Connor stressed that caveats are important and should be respected. Commissioner Iacobucci's recent report also reached this conclusion. However, Canada is not without a remedy. It can ask that caveats be lifted to facilitate a terrorism prosecution in Canada. Commissioner O'Connor wrote:

> Caveats should not be seen as a barrier to information sharing, especially information sharing beyond that contemplated on their face. They can easily provide a clear procedure for seeking amendments or the relaxation of restrictions on the use and further dissemination of information in appropriate cases. This procedure need not be time-consuming or complicated. With the benefit of modern communications and centralized oversight of information sharing within the RCMP, requests from recipients should be able to be addressed in an expeditious and efficient manner.[108]

Canada has adequate tools, including non-disclosure orders under section 38.06 of the *Canada Evidence Act*, non-disclosure certificates issued by the Attorney General of Canada under section 38.13 and stays of prosecution, to ensure that the caveats are respected.

Justice Mosley of the Federal Court recognized the importance of the third party rule in promoting "…the exchange of sensitive information between Canada and foreign states or agencies." He stated that, under the rule, Canada should not release information or even acknowledge its source without the consent of the original provider. He noted that, nevertheless, the third party rule was "…not all encompassing….[I]t is not open to the Attorney General to merely claim that information cannot be disclosed pursuant to the third party rule, if a request for disclosure in some form has not in fact been made to the original foreign source."[109] These statements recognize the importance of asking allies to consider lifting caveats to allow the further disclosure of secret information. Such requests are particularly important because the circumstances that originally led the third party to restrict disclosure – such as a concern that disclosure

---

108 *Report of the Events Relating to Maher Arar: Analysis and Recommendations*, p. 339.
109 *Canada (Attorney General) v. Khawaja*, 2007 FC 490, 219 C.C.C. (3d) 305 at paras. 145-146.

might compromise an ongoing intelligence operation of the third party – may disappear by the time a Canadian terrorism prosecution begins.

Justice Mosley also recognized that the third party rule should not apply "… where a Canadian agency is aware of information prior to having received it from one or more foreign agencies" or where the information is in the public domain and can be disclosed "…so long as it is the public source that is referenced."[110] The requirement that the originator of secret information be asked to modify a caveat, and that the third party rule should not apply to information that Canada has obtained independently or that is already in the public domain, are important changes to the third party rule.

Unfortunately, there are signs that the practices of agencies and of the Attorney General of Canada have not fully accepted this evolution of the third party rule in their approach to secrecy. This was illustrated when an affidavit was introduced in a recent case stating that, "…if the RCMP were to seek consent to disclose the information in this case, the RCMP's commitment to the third-party rule may be questioned as disclosure would be sought for a purpose other than law enforcement, and therefore outside the general accepted parameters for seeking consent."[111]

Requests to amend caveats in fact affirm Canada's commitment to the third party rule by acknowledging that disclosure is not allowed without the originating party's consent. A third party that provided the information to Canada could refuse to amend the caveat, and Canada would honour that request. In short, it does not hurt to ask, and it is necessary to do so.

Another part of the national security confidentiality jurisprudence is evolving to reflect the changed threat environment. There is increasing judicial skepticism about arguments that innocuous pieces of information should not be disclosed because of the "mosaic effect." The mosaic effect describes a belief that, by assembling into a "mosaic" bits of information that are innocuous by themselves, a hostile party might acquire more comprehensive knowledge that can be used to harm national security. In a recent case, the Attorney General of Canada relied on an affidavit by a CSIS officer that claimed that, "…in the hands of an informed reader, seemingly unrelated pieces of information, which may not in and of themselves be particularly sensitive, can be used to develop a more comprehensive picture when compared with information already known by the recipient or available from another source."[112] However, the lack of evidence that this has occurred left this Commission skeptical about the validity of the "mosaic effect" concept.

---

110 2007 FC 490, 219 C.C.C. (3d) 305 at para. 147.

111 As described in *Canada (Attorney General) v. Canada (Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar)*, 2007 FC 766, 319 F.T.R. 279 at para. 72.

112 As quoted in *Canada (Attorney General) v. Canada (Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar)*, 2007 FC 766, 319 F.T.R. 279 at para. 83.

Other countries seem more reluctant than Canada has been to date to restrict disclosure on the basis of the "mosaic effect" argument. Canadian courts are now becoming more reluctant to accept the mosaic effect as the sole reason for refusing the disclosure of information. Justice Mosley concluded that, "… by itself, the mosaic effect will usually not provide sufficient reason to prevent the disclosure of what would otherwise appear to be an innocuous piece of information. Something further must be asserted as to why that particular piece of information should not be disclosed."[113] If the Attorney General of Canada wants to restrict disclosure on the grounds that disclosure would harm national security, he is entitled to do so.

The current Federal Prosecution Service Deskbook chapter on national security confidentiality has apparently not been revised since 2000.[114] The Director of Public Prosecutions should revise this material to reflect the developments in the case law that were described earlier. In particular, the revisions should reflect the call for Canada to request third parties to lift caveats restricting the disclosure of information, rather than allowing Canada simply to rely on the original caveat. The revisions should also note that the mosaic effect should not be the sole basis for a national security confidentiality claim. More generally, the Attorney General of Canada should exercise independent judgment when making secrecy claims and not be swayed by the various agencies.

The Attorney General of Canada should avoid overly broad claims of harm to national security. As Commissioner O'Connor stressed, making overly broad secrecy claims serves nobody's interests.[115] Over-classification of information – giving a security classification that is higher than warranted – and overstating the need for secrecy actually increase the threat to national security by making it more difficult to share vital information.

The Air India investigation demonstrated how excessive secrecy impeded the state in preventing terrorism. Claims of secrecy also make terrorism prosecutions more difficult. Increased discipline is necessary in making secrecy claims.

The Director of Terrorism Prosecutions – a position proposed in Chapter III – should play a central role in handling claims of national security confidentiality. Lawyers from the Director's office would be in a position to see the problem in the context of the complex relationship between intelligence and evidence and the difficult trade-offs between secrecy and disclosure. They could offer continuity of legal advice.

The Director of Terrorism Prosecutions should be in a position to understand the perspective of CSIS, with its frequent concerns about the disclosure of

---

113 *Canada (Attorney General) v. Khawaja*, 2007 FC 490, 219 C.C.C. (3d) 305 at para. 136. See also *Canada (Attorney General) v. Canada (Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar)*, 2007 FC 766, 319 F.T.R. 279 at para. 84.

114 As suggested by the Table of Contents, online: Department of Justice Canada <http://www.justice.gc.ca/eng/dept-min/pub/fps-sfp/fpd/toc.html> (accessed July 30, 2009).

115 *Report of the Events Relating to Maher Arar: Analysis and Recommendations*, p. 304.

intelligence, as well as the perspective of the RCMP and other police forces that need admissible evidence to support prosecutions. The Director should be able to understand how overly broad claims of secrecy can hinder a terrorism prosecution. This appreciation of the larger picture may be lacking under the present system, where one group of lawyers represents the Attorney General of Canada in making section 38 claims, and another group – federal or provincial – conducts prosecutions.

Whichever official makes national security confidentiality claims on behalf of the Attorney General of Canada should exercise independent judgment in order to limit the potential for overly broad claims by respective agencies. Such claims must be made in a manner that respects the Attorney General's tradition of pursuing the public interest.[116]

7.9 The Ultimate Responsibility of the Attorney General of Canada with Respect to Disclosure of Intelligence

Several witnesses testified about the uncertainty created by the combination of broad disclosure rules and the lack of jurisprudence under section 38 of the *Canada Evidence Act*. Former RCMP Commissioner Giuliano Zaccardelli testified that this uncertainty affected the RCMP's dealings with its partners, and that that he "totally" agreed that "CSIS has every right to be concerned about what happens when they release some information and it goes into the disclosure pipeline because none of us can control it; that's a legitimate concern." He added that the lack of a guarantee also affected relations with international partners, "…which we need more and more every day because the threats we face transcend all of us…whether they be in the national security area or in the organized crime area."[117] An earlier RCMP Commissioner, Norman Inkster, similarly testified that, in his experience, the RCMP could not give "iron-clad" guarantees of non-disclosure, and that some foreign agencies decided that section 38 was simply not a sufficient guarantee that information they supplied would be protected from disclosure.[118]

There is a vehicle to protect against disclosure. The Attorney General of Canada has the authority under section 38.13 of the *Canada Evidence Act* to issue a certificate personally prohibiting the disclosure of information, even in the event that a judge has made an order for disclosure. This provision was added in 2001 by the *Anti-terrorism Act*, and is subject to limited judicial review.[119]

The personal certificate of the Attorney General is the ultimate protection against the disclosure of intelligence. The certificate places responsibility for

116 *Krieger v. Law Society of Alberta*, 2002 SCC 65, [2002] 3 S.C.R. 372.
117 Testimony of Giuliano Zaccardelli, vol. 86, November 30, 2007, p. 11037.
118 Testimony of Norman Inkster, vol. 81, November 22, 2007, pp. 10329-10330.
119 A single judge of the Federal Court of Appeal hears applications for an order varying or cancelling the certificate. The judge cancels the certificate if he or she determines that none of the information was obtained in confidence from or in relation to a foreign entity or to national defence or national security: *Canada Evidence Act*, ss. 38.131(1), (4), (9).

protecting secrets on the shoulders of an accountable official who can strike his or her own balance between the demands of secrecy and disclosure.

Although the Attorney General's authority to issue a certificate has generated controversy, the certificate has value as a safeguard that allows the Attorney General to prevent the disclosure of intelligence against the wishes of a foreign government. Neither CSIS nor the RCMP can provide that kind of guarantee.

When deciding whether to issue a non-disclosure certificate, the Attorney General can consult the National Security Advisor and other officials. However, the Attorney General must decide independently whether the public interest requires a non-disclosure certificate.

No Attorney General of Canada has yet issued a non-disclosure certificate under section 38.13. It is understandable that the Attorney General will use this extraordinary power cautiously. The Attorney General should consider using this certificate when it is necessary to honour promises made to allies that intelligence will not be disclosed.

Recommendation 22:

The Attorney General of Canada, through the proposed Director of Terrorism Prosecutions, should exercise restraint and independent judgment when making claims under section 38 of the *Canada Evidence Act* and avoid using overly broad claims of secrecy.

Recommendation 23:

The Federal Prosecution Service Deskbook and other policy documents that provide guidance about making secrecy claims should be updated to encourage the making of requests to foreign agencies to lift caveats that they may have placed on the further disclosure of information. These documents should also be updated to reflect the evolution of national security confidentiality jurisprudence. In particular, the Deskbook should direct prosecutors to be prepared to identify the anticipated harms that disclosure would cause, including harms to ongoing investigations, breaches of caveats, jeopardy to sources and the disclosure of secret methods of investigations. The Deskbook should discourage reliance solely on the "mosaic effect" as the basis for making a claim of national security confidentiality.

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

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

8.0 Introduction

The terms of reference for the *Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182* require the Commissioner to make findings and recommendations with respect to "…whether existing practices or legislation provide adequate protection for witnesses against intimidation in the course of the investigation or prosecution of terrorism cases."[1]

The analysis that addresses this part of the Commission's mandate is included in this volume because of the critical importance that witness protection plays in terrorism prosecutions.[2] In addition, protecting witnesses from intimidation is an important means to improve the relationship between secret intelligence and public evidence. The adequacy of witness protection is often influential in deciding whether secret human sources should testify and provide evidence in public trials. Witness protection may also be necessary where identifying information about an informer is disclosed, even when that informer does not testify.

The terms of reference do not call for the Commissioner to reach conclusions specifically about the intimidation of witnesses involved in the investigation of the bombing of Air India Flight 182, and this report does not do that. However, the Commission received evidence on this point, and this evidence provided the background for the assessment of the challenges of witness protection in terrorism prosecutions.

The requirements for witness protection may create the impression that the witness is the beneficiary. In fact, it is the members of the public who benefit. This

---

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

2 Professor Yvon Dandurand prepared a paper on this topic for the Commission: "Protecting Witnesses and Collaborators of Justice in Terrorism Cases" in Vol. 3 of Research Studies: Terrorism Prosecutions [Dandurand Paper on Protecting Witnesses]. Professor Bruce Hoffman also touched on intimidation of witnesses and witness protection in his testimony and in a paper he prepared for the Commission: "Study of International Terrorism" in Vol. 1 of Research Studies: Threat Assessment RCMP/CSIS Co-operation [Hoffman Paper on International Terrorism].

is particularly true with terrorism, where murder and mayhem are indiscriminate. It is principally to protect innocent Canadians that witness protection must be as efficient and secure as possible. If Canada can improve witness protection measures, those with information vital to public safety will be more likely to disclose it and, when necessary, testify.

8.1 Terminology

Several terms are used in the legal and social sciences literature to describe individuals who help authorities with investigations and prosecutions. These terms are used imprecisely, confusing the discussion about the status and rights of the individuals, the type of assistance they are providing and the extent of their need for protection from retaliation. Broad statutory definitions can add further confusion. For example, a witness is defined for the purpose of the *Witness Protection Program Act* as both a person who has agreed to give evidence and a person who has already given information, as well as any close relative who may require protection.[3]

The commonly described "informer" could be one of several different participants in the justice system:

- A person who hears about a terrorist plot and passes the information to police (a police informer) or intelligence authorities, but does not testify at a subsequent trial. This individual can also be called a "source;"
- A criminal or other individual directed by the proper authorities to infiltrate an organization (police agent) and perhaps try to influence events (possibly becoming an *agent provocateur*[4]);
- A material witness[5] – a witness who can testify to material facts,[6] as well as someone considered a "crucial" witness;[7] and
- An individual who eventually testifies at trial as a witness.

In this chapter, the term "informer" is used interchangeably with "source." An informer refers to an individual who provides information to authorities, but who does not qualify as a police agent, *agent provocateur*, material witness or witness at trial.

---

3 Section 2 of the *Witness Protection Program Act*, S.C. 1996, c. 15 [*Witness Protection Program Act*] defines a "witness" as: (a) a person who has given or has agreed to give information or evidence, or participates or has agreed to participate in a matter, relating to an inquiry or the investigation or prosecution of an offence and who may require protection because of risk to the security of the person arising in relation to the inquiry, investigation or prosecution, or (b) a person who, because of their relationship to or association with a person referred to in paragraph (a), may also require protection for the reasons referred to in that paragraph.

4 *R. v. Scott*, [1990] 3 S.C.R. 979 at 996.

5 *R. v. Scott*, [1990] 3 S.C.R. 979 at 996.

6 *Lemay v. The King*, [1952] S.C.R. 232 at 242.

7 As was "Billy Joe" in *R. v. Khela*, [1995] 4 S.C.R. 201.

There is a need for precision when referring to individuals who provide information, since different rules apply depending on the nature of the individual's involvement. The identity of a police informer cannot be disclosed to an accused in a criminal trial because of the "police informer privilege" exception in criminal law. The only time this privilege does not apply is when the innocence of the accused is at stake.[8] However, if the person is actually operating under the direction of the police, the person is then a police *agent*, not an informer, and the person's identity would, subject to some exceptions, have to be disclosed. Similarly, the identity of an *agent provocateur* and a material witness generally need to be disclosed. As discussed in Chapter VI, it is not clear that a CSIS source enjoys the benefit of police informer privilege.

This chapter focuses on witnesses who are expected to testify and whose identity will normally be disclosed. In some cases, however, sources who do not testify may also need protection because of the risk that they can be identified by their adversaries. In addition, protection may be necessary as a precautionary measure because it may not be clear whether the identity of the source will eventually be protected by police informer privilege.

8.2 Why Witness Protection

A failure to provide adequate protection for witnesses threatens their safety and, sometimes, their lives. It discourages others from helping intelligence or police agencies. In the end, poorly designed witness protection measures can rob the justice system of crucial assistance.

Witness protection, both for witnesses who testify and for sources who provide information, is examined here. The focus on both witnesses and sources is necessary to ensure that sources can sometimes be developed into witnesses able to provide evidence in terrorism prosecutions. The examination of both witnesses and sources is also necessary to ensure that valuable sources are not lost because of ineffective attempts to have them testify. It may be possible for a source developed by CSIS to become a witness in a terrorism prosecution, and such transitions can be seen as part of the intelligence/evidence relationship discussed throughout this volume.

Witness protection that encourages people with information to come forward involves physical protection against retribution and other measures designed to protect and comfort them while under witness protection. This enhances their trust in intelligence and police agencies and creates an environment where important information is likely to flow more freely to the authorities. Witness protection also involves developing a "culture of security" within the institutions that reflects an awareness of the real risks to those who assist the authorities in guarding against terrorism.[9]

---

8 See *Named Person v. Vancouver Sun*, 2007 SCC 43, [2007] 3 S.C.R. 252 at paras. 27-30 and Section 8.4.3.

9 Testimony of Anne-Marie Boisvert, vol. 69, October 30, 2007, pp. 8771-8773.

Early witness protection programs in Canada were designed to deal with informers and witnesses in organized crime cases.[10] Too little thought has gone into witness and source protection in terrorism investigations and prosecutions – an environment that can have very different witness protection needs and challenges. As the investigation into the Air India tragedy showed, the RCMP viewed witnesses and sources in terrorism matters in the same way that it had viewed them in ordinary criminal investigations. This lack of appreciation of the difference between witnesses and sources in ordinary criminal cases and those in terrorism cases also resulted in insensitive approaches by the RCMP to those involved in the Air India tragedy. This placed them at risk and created a distrust of law enforcement.

Many potential witnesses in terrorism prosecutions may already have been confidential sources for CSIS. Since the eligibility of CSIS sources to claim informer privilege is not clear, it is also not clear whether a CSIS handler can make a promise of anonymity. Care must be taken to avoid making unrealistic promises of permanent anonymity to sources. Sources must be sensitively and adequately prepared for the possibility that they may have to testify in some cases. In addition, there is a need for both CSIS and the RCMP to understand and accommodate the difficulties of converting intelligence sources into witnesses.

Also missing from witness protection to date is a consideration of the measures which lie between providing complete anonymity and fully disclosing identity. These include protections available under sections 37 and 38 of the *Canada Evidence Act*[11] and partial anonymity at trial through the use of pseudonyms, screens or remote testimony. The possibility of allowing anonymous testimony at a criminal trial is also explored.

The Commission has concluded that police, intelligence agencies, prosecutors and judges should explore the full range of these measures. If the measures are not appropriate (for example, if prosecutors determine that testimony in open court is essential), the government should provide appropriate protection measures, including formal witness protection programs attuned to the sometimes unique needs of witnesses in terrorism cases.

This chapter examines the characteristics of terrorism that may impede the recruitment of witnesses and sources. It discusses both specific and "community-wide" intimidation, and how genuine fear in some communities, combined with the cultural insensitivity of the authorities approaching members of those communities, makes it difficult to persuade individuals to share valuable information about terrorist activities. There is an examination of means other than formal witness protection programs to protect individuals who assist the authorities. The emphasis is on developing a range of graduated and appropriate strategies to protect witnesses. The notion that "one size fits all"

---

10 See Gregory Lacko, "The Protection of Witnesses" (Ottawa: Department of Justice, 2004), p. 3, online: Department of Justice Canada: <http://www.justice.gc.ca/eng/pi/icg-gci/pw-pt/pw-pt.pdf> (accessed June 2, 2009) [Lacko Paper on Protection of Witnesses].

11 R.S.C. 1985, c. C-5.

when protecting witnesses and sources is unrealistic, particularly in the unique context of international terrorism investigations.

The existing federal Witness Protection Program (WPP), developed largely to protect witnesses in criminal prosecutions, cannot easily be transplanted to the terrorism environment. The management of the Program, as well as several other aspects of it, must change significantly – as must the attitudes of police and intelligence agencies dealing with witnesses and sources. This chapter recommends a new national security witness protection program separated from RCMP control. It would be headed by a respected independent individual to be known as the National Security Witness Protection Coordinator. The Coordinator would determine qualifications, requirements and approval of candidates for acceptance into the Program. The Coordinator would be able to seek advice, when appropriate, from various agencies including CSIS, the RCMP, the office of the proposed Director of Terrorism Prosecutions and other prosecutorial officials, Corrections Canada, immigration officials and others. The Coordinator should consult, but he or she would make the final decisions.

The Coordinator would be responsible for making arrangements for protection while the person is in the program and for resolving disputes that may arise between the protectee and the program. In some cases, the Coordinator should be prepared to justify unpopular arrangements that were made for valid reasons of witness and source protection. The Coordinator would act in the public interest and be independent of the police and prosecutors. He or she would have the power to devise creative and flexible solutions to the varied problems of witness and source protection in terrorism investigations. The Coordinator could also act as a resource for the agencies and the National Security Advisor on witness and source protection issues.

Removing from the RCMP the authority to decide who qualifies for witness protection avoids the perception of conflict of interest. The inference that arises when the RCMP has that authority is obvious: "Co-operate with the RCMP, say what is required and we at the RCMP will decide if you qualify for protection." Such a conflict of interest can damage perceptions about the credibility of a witness who is in witness protection. The National Security Witness Protection Coordinator would be able to avoid the conflict of interest between witness protection and policing/prosecutorial interests. However, the Coordinator would receive input from the RCMP and the RCMP would continue, when appropriate, to provide actual protection to the witness.

The conflict between policing/prosecutorial interests and the protection of witnesses would be similar in other criminal cases. However, the terms of reference restrict the Commission's recommendations to the problems of witness protection in terrorism cases. In addition, witness and source protection in terrorism investigations can give rise to a need for ethnic, cultural, religious and linguistic sensitivity that may not be necessary in ordinary criminal cases. There may also be more of an international dimension to witness and source protection in some terrorism investigations.

8.3 Witness Intimidation and its Impact on Terrorism Investigations and Prosecutions

8.3.1 The Context of Terrorism

In his testimony, Professor Yvon Dandurand of the University of the Fraser Valley described how international terrorist groups have increasingly turned for support to overseas communities:

> [I]f you look at studies in the last 20 years on the evolution of terrorist movements, one of the characteristics that experts normally isolate is the fact that more and more international terrorist groups have found effective ways of obtaining support from diasporas and from ethnic groups, in different countries, that either are sympathizers or are not sympathizers but fall under the influence of these radical groups.[12] [translation]

For this reason, Dandurand argued, the assistance of members of these communities is essential for preventing and prosecuting terrorist activity:

> [I]t is absolutely essential that we be able to count on the cooperation of the communities within which terrorist groups have a tendency to hide. We must therefore work very closely with those communities.[13] [translation]

Unfortunately, some of the communities with the greatest potential to assist the authorities in terrorism investigations and prosecutions also often face the greatest barriers to providing that assistance. Among those barriers is the fear of intimidation against community members who cooperate or speak out against extremists. Other significant barriers to providing assistance include a distrust of the authorities and the distance and alienation of these communities from broader Canadian society. These barriers are discussed below.

8.3.2 Exploiting the Particular Vulnerabilities of Some Communities – "Community-wide" Intimidation

To assert their power, terrorists threaten, intimidate or attack those who cooperate against them. This has a three-pronged effect: exacting revenge on individuals, reducing the chances of a successful prosecution and discouraging others from helping the authorities.

Members of some minority communities who assist the authorities in terrorism investigations can face significant risks if their assistance becomes known to

---

12 Testimony of Yvon Dandurand, vol. 68, October 29, 2007, p. 8576.
13 Testimony of Yvon Dandurand, vol. 68, October 29, 2007, p. 8566.

extremists. These communities can be so close-knit that cooperation with investigators is readily noticed. Individuals who are exposed fear violence, ostracism by the community, or both.

They are also vulnerable to a less common type of intimidation – "community-wide" intimidation. This involves "…acts that are intended to create a general sense of fear and an attitude of non-cooperation with police and prosecutors within a particular community."[14] Intimidation can be experienced by individuals who have not been directly or personally threatened, but who are aware that any member of their community who is seen as assisting the authorities is likely to face reprisals. Community-wide intimidation can also help to silence those who simply oppose extremist agendas and rhetoric.

Dandurand stated in his report for the Commission that community-wide intimidation is especially frustrating for the police and prosecutors because, even if no actionable threat is made, witnesses and victims are still effectively discouraged from testifying.[15] As he explained:

> Terrorist groups and criminal groups make very organized efforts to convey … to communities, the message that, if someone from the community decides to work with the authorities, there will be highly unpleasant consequences for that person. They do this systematically; they constantly reinforce the message. And so the people who live in these communities know it even though it is not always necessary to make explicit threats. [translation]

Dandurand elaborated on his analysis in his testimony:

> ... [R]umours are spread in the community, veiled threats are made, metaphors and so forth are used to spread the message that people who work with the authorities do so at their own risk and peril, and this message is usually buttressed by striking examples that will ignite community members' imaginations. So an example is made of one or two people who, for instance, came out publicly against a movement or against certain individuals involved in a conspiracy or a radical group, and they are made examples of by violence or ostracism.[16] [translation]

---

14 Dandurand Paper on Protecting Witnesses, p. 30, citing K. Dedel, *Witness Protection* Problem-Oriented Guides for Police Series, No. 42 (Washington, D.C.: United States Department of Justice, Office of Community Oriented Policing Services, 2006), p. 4.

15 Dandurand Paper on Protecting Witnesses, p. 31; Testimony of Yvon Dandurand, vol. 68, October 29, 2007, pp. 8565-8566.

16 Testimony of Yvon Dandurand, vol. 68, October 29, 2007, pp. 8568-8570.

For ostracism to be a meaningful threat, individuals must also view their community as distinct from the wider society, and they must see the wider society as antagonistic to their community. Being ostracized would mean being left to fend alone.

Dandurand told the Commission that criminal organizations and some terrorist groups are sophisticated enough to present themselves to some communities as protectors. He called this tactic "…a very effective method of keeping a community under control."[17] Intimidation and indoctrination work together. "[V]ulnerable, disenfranchised, or segregated communities," he argued in his research paper, were susceptible to "low-level community-wide intimidation" by either organized criminals or radical groups:[18]

> It is apparently often the case that ethnic communities living in ethnic enclaves are less inclined to integrate with their host societies and thus become more susceptible to insurgent indoctrination and vulnerable to intimidation by terrorists and other criminals. Anything that contributes to the isolation or ghettoization of these groups increases the likelihood that they could be intimidated, victimized, recruited or exploited by criminal or terrorist organizations.[19]

Dandurand also emphasized that creating a sense of vulnerability among members of these communities is important for criminal and terrorist groups:

> Criminal groups often go to great lengths to maintain their victims in a constant state of vulnerability and powerlessness. This is often the case, for example, with illegal immigrants illegally smuggled into the country and potentially subject to deportation. Their vulnerability to deportation can be purposefully manipulated and exploited by terrorist groups.
>
> …
>
> ... Anything that contributes to the further alienation and isolation of these individuals can indirectly facilitate their exploitation by terrorist groups. Furthermore, these illegal residents/immigrants normally have strong and immediate ties to other members of the same immigrant community. What happens to them and how they are treated can also contribute to feelings of alienation, exclusion and vulnerability within the community as a whole. Criminal and terrorist groups are of

17 Testimony of Yvon Dandurand, vol. 68, October 29, 2007, p. 8590.
18 Dandurand Paper on Protecting Witnesses, p. 31.
19 Dandurand Paper on Protecting Witnesses, p. 42.

> course known to blackmail illegal residents and their relatives (even if they are themselves legal residents) by threatening to denounce them to the authorities. [20]

Dandurand suggested that threats against family members overseas can be credible and effective means of intimidation.[21]

A March 2006 Human Rights Watch report[22] offered examples of intimidation of members of overseas communities. The report detailed the alleged intimidation of Tamil communities in Canada, the UK and other countries by the Liberation Tigers of Tamil Eelam (LTTE, or Tamil Tigers). The report claimed that the LTTE, besides pressuring individuals to donate to charitable organizations linked to the LTTE, used several intimidation tactics to silence dissent:

> Tamils in the West have been subject to death threats, beatings, property damage, smear campaigns, fabricated criminal charges, and even murder as a consequence of dissent. Although incidents of actual violence have been relatively rare, they reverberate strongly within the community and effectively discourage others from expressing views that counter the LTTE.[23]

This phenomenon of community-wide intimidation is widespread, and perhaps growing, outside the context of terrorism. William Blair, Chief of the Toronto Police Service, attributed many unsolved crimes to this type of intimidation. Witnesses were unwilling to come forward in criminal investigations, he testified, because they expected criminal gangs to be informed quickly of their cooperation with police:

> And what they complain to us is … that the accused and all of his friends and everyone in their neighbourhood will know that they were the one that came forward with information and from that point on, they're in danger; from that point on, their children can't go to the same schools as their neighbours; that their reputation in the community is destroyed…. In some cases, their statements are being handed around the neighbourhood because we'd given them to a defence lawyer who has given them to the accused who has handed them out, just to show to his other gang members or his neighbours and

---

20 Dandurand Paper on Protecting Witnesses, pp. 41-42.

21 Dandurand Paper on Protecting Witnesses, pp. 41-42. See also Testimony of Isabelle Martinez-Hayer, vol. 76, November 15, 2007, pp. 9534-9535.

22 Jo Becker, *Funding the 'Final War*: LTTE Intimidation and Extortion in the Tamil Diaspora" *Human Rights Watch* (March 2006), online: Human Rights Watch <http://hrw.org/reports/2006/ltte0306/ltte0306webwcover.pdf> (accessed June 2, 2009) [Becker Paper on LTTE]. See also the discussion of LTTE coercion and fundraising in Hoffman Paper on International Terrorism, pp. 43-44.

23 Becker Paper on LTTE, p. 14.

> friends that this is the person who has been a witness against him.… They don't trust us and they don't cooperate with us. And they tell their neighbours and their friends and their children not to trust us either.[24]

8.3.3 How Distrust and Distance Limit the Ability of Authorities to Provide Protection

The distance and distrust between police and intelligence agencies and communities can increase reluctance to cooperate with authorities and heighten the sense of vulnerability flowing from intimidation tactics. Several factors may contribute to this distance and distrust:

As Dandurand stated in his research paper:

> Counter-terrorism strategies do not typically address the need to offer active protection to these vulnerable groups. A legalistic/instrumentalist approach to this question tends to prevail. As a result, the services of State protection programs are extended to victims of intimidation and exploitation in their capacity as witnesses and informants, but only to the limited extent that their participation is required by the justice system itself. Otherwise, intimidated individuals tend to be left to their own devices.[25]

Dandurand argued that investigative hearings[26] previously permitted by the *Criminal Code*[27] "…clearly add to the already existing feelings of vulnerability and insecurity of members of vulnerable groups. They also convey a conflicting message by suggesting to those with information about potential terrorists that volunteering it to the authorities could result in their finding themselves subject to an investigative hearing, a preventive arrest or a charge under a broad array of new terrorism offences."[28]

- Distrust may also arise when police or intelligence agencies are not faithful to their promises – particularly promises to keep the identity of sources secret. Other times, authorities may not be open about legal obligations to disclose the identity of

---

24 Testimony of Wiliam Blair, vol. 78, November 19, 2007, pp. 9996-9998.

25 Dandurand Paper on Protecting Witnesses, p. 44. See also Testimony of Ujjal Dosanjh, vol. 80, November 21, 2007, p. 10168.

26 Investigative hearings, a procedure introduced by the *Anti-terrorism Act*, S.C. 2001, c. 41, allowed a court to issue an order for the gathering of information from a named individual. The power to order investigative hearings ended in 2007 because of a "sunset" clause in the legislation. A bill to revive these hearings, Bill S-3, died on the Order Paper when Parliament was dissolved for the October 2008 election: Bill S-3, *(An Act to amend the Criminal Code (investigative hearing and recognizance with conditions)*, 2nd Sess., 39th Parl., 2007-2008.)

27 R.S.C. 1985, c. C-46.

28 Dandurand Paper on Protecting Witnesses, pp. 43-44.

the source. Distrust may arise even if the police truly want to keep someone's identity secret, but are forced to reveal it by disclosure rules. As Blair testified, "[I]t doesn't do that I tell them that I was required by law to do it. They don't understand that. They don't trust us and they don't cooperate with us."[29]

- Community members may distrust these agencies because of experiences with similar organizations in their countries of origin. They may associate the authorities with corruption, predatory behaviour and incompetence. In some communities, Dandurand testified, the idea that police officers are there to help and protect would be radical.[30]

- Even if there is no distrust of authority among community members, there may be an *absence* of trust in intelligence and police agencies simply because those agencies are not well-established in the communities, often do not understand their dynamics and appear unwilling to help. For example, Dandurand told the Commission that "…a number of threats, means of intimidation, are delivered secretly, in code or veiled words, by metaphors and so forth. Thus, someone with only a superficial knowledge of the culture would often find it very hard to decode threats, decode conversations."[31] [translation] Former police officer Mark Lalonde described another circumstance where "ethnic radio" could broadcast a threat that was well understood by the targetted audience but would not be interpreted as such by the public at large. The message would not violate any laws, so no police intervention would occur. However, the targeted groups would interpret this as the police being "unwilling or unable to respond."[32]

8.3.4 Examples of Individual and Community-wide Intimidation in the Air India Context

Both the judgment of Justice Josephson in *R. v. Malik and Bagri*[33] and evidence before the Commission were replete with descriptions of attempted and successful intimidation.

In 2004, Justice Josephson ordered a permanent publication ban relating to the identity of one witness, Ms. E, at the Air India trial. He spoke of the serious threat to the lives of Ms. E and her family:

---

29 Testimony of William Blair, vol. 78, November 19, 2007, p. 9997.
30 Testimony of Yvon Dandurand, vol. 68, October 29, 2007, pp. 8585-8586.
31 Testimony of Yvon Dandurand, vol. 68, October 29, 2007, p. 8572.
32 Testimony of Mark Lalonde, vol. 68, October 29, 2007, pp. 8630-8631.
33 2005 BCSC 350.

> There is evidence of threats and violence being directed towards those who have taken contrary positions to those of certain extremist elements. There is also evidence of what the Witness not unreasonably interpreted to be a serious threat to the lives of herself and her family should she reveal certain information. Only upon receiving an assurance that her identity would remain confidential did she disclose this information to the authorities, maintaining throughout that she would never testify out of fear for the safety of herself and her family.
>
> In this context, the Witness's ongoing security concerns rise beyond the merely speculative. The risk also does not abate simply because she has completed her testimony, as retaliation is a strong element of the risk.[34]

Ms. E was a former friend of Ajaib Singh Bagri who provided statements to CSIS and the RCMP in the years following the Air India tragedy. A former CSIS agent testified at trial that Ms. E had told him of a threat by Bagri. Bagri had allegedly said that they shared secrets and that she knew what he would do if she told anyone. According to the CSIS agent, Ms. E indicated that she was certain that Bagri meant that he would kill her.[35] The CSIS agent testified before the Commission to the same effect.[36]

Several threats were also made against a Ms. D and her family. From the beginning of her dealings with the authorities, Ms. D indicated that she had been the victim of threats and intimidation and that she feared for her safety.[37] Early in November 1997, the RCMP installed a video surveillance camera at Ms. D's residence.[38] Ms. D continued to receive threats after she began speaking with the RCMP.

On February 14, 1998, Ms. D was warned by a relative of Balwant Bhandher to be careful because three men, Ripudaman Singh Malik, Bhandher and Aniljit Singh Uppal, had met and would "…try to shut her up permanently."[39] Shortly after, she was approached at a Sky Train station and told by a young East Indian male that Malik would "finish" her and reporter Kim Bolan.[40] In March 1998, eggs were thrown at her house in the middle of the night and she received a number of unsettling phone calls.[41] In June 1998, Ms. D was at a shopping centre with her child when a former acquaintance from the Khalsa School where she had worked

---

34 *R. v. Malik and Bagri*, 2004 BCSC 520 at paras. 6-7.
35 *R. v. Malik and Bagri*, 2005 BCSC 350 at paras. 960, 980.
36 Testimony of William Laurie, vol. 61, October 15, 2007, pp. 7411-7412.
37 *R. v. Malik and Bagri*, 2005 BCSC 350 at paras. 380, 396.
38 2005 BCSC 350 at paras. 377, 414.
39 2005 BCSC 350 at para. 352.
40 Exhibit P-101, CAF0485, p. 1.
41 Exhibit P-101, CAF0485, p. 3.

approached her and warned her that she was creating a lot of problems.[42] The individual was aware of personal information about Ms. D's child and warned her that she and her family would be severely harmed if she did not "watch it."[43]

In July 1998, Kim Bolan contacted the RCMP and advised that she had received information about a "hit list" and had been told that a person from the US would come with AK-47s "…to take care of the hit list."[44] Ms. D's name, as well as those of Tara Singh Hayer and Ms. Bolan herself, were reportedly included on the list.[45] At the time, Bolan, who had heard a gun shot on her street on July 16, reported to the RCMP her belief that the person from the US and the AK-47s were "… already in town to carry out the hit list contract."[46] As a result of the "hit list" information, an additional video surveillance camera was installed at Ms. D's residence by the RCMP.[47]

Justice Josephson's 2005 judgment in *R. v. Malik and Bagri* noted that Ms. D "… continues to have constant concerns about her safety and security."[48]

The Commission learned of other examples of feared intimidation or actual intimidation and retaliation:

> **Mr. A**: A former CSIS officer told the Commission about his relationship with a Mr. A. Mr. A had been providing information to CSIS in confidence but was very reluctant to deal with the RCMP because he feared for his personal safety if he had to lose his anonymity and testify.[49] The former CSIS officer testified that Mr. A's fear was a "…very legitimate concern ... for sure."[50]
>
> **Tara Singh Hayer**: Hayer was the publisher of the *Indo-Canadian Times* and an outspoken critic of extremism. He also provided information to CSIS and then to the RCMP about the Air India bombing. An attempt on his life left him paralyzed in 1988. The BC Crown later alleged that the attempt related to his knowledge about Air India. He was murdered in 1998. Those responsible for his murder were never caught.[51]

8.3.5 Intimidation of Members of the Sikh Community for "Speaking Out"

Beyond intimidation of specific individuals involved in the investigation of the Air India case, community-wide intimidation was at play against those who

42 *R. v. Malik and Bagri*, 2005 BCSC 350 at para. 352.
43 2005 BCSC 350 at para. 352.
44 Exhibit P-101, CAF0485, p. 3.
45 Exhibit P-101, CAF0485, p. 3.
46 Exhibit P-101, CAF0485, p. 3.
47 Exhibit P-101, CAF0485, p. 5.
48 *R. v. Malik and Bagri*, 2005 BCSC 350 at paras. 352-353.
49 Exhibit P-291: "Mr. A Agreed Statement," pp. 25-26.
50 Testimony of Neil Eshleman, vol. 75, November 14, 2007, p. 9449.
51 See Volume Two, Part 2, Post-Bombing, Section 1.2, Tara Singh Hayer.

might want to speak out against extremism. In his 2005 report, the Hon. Bob Rae described how family members of Air India Flight 182 victims perceived a "culture of fear" within communities that prevented people from telling the truth about what had happened.[52] That culture of fear was reinforced by specific acts of violence and extended beyond intimidation of witnesses to the suppression of community opposition to extremist agendas.[53]

Tara Singh Hayer's son, David ("Dave") Hayer, a Member of the BC Legislative Assembly, told the Commission how his father's opposition to Sikh violence in the aftermath of the Air India bombing resulted in an attempt to bomb his father's office, numerous threats, and an attempt on his life in 1988.[54]

Dave Hayer also testified about the fearful atmosphere in the Sikh community in 1986-87:

> I think everybody was afraid and if you said anything that did not support the cause of the people who were trying to support terrorism and violence, a state of -- independent State of India, you will be called names and you will -- on the radio stations you will be called outside. They will go to Sikh temples. They had basically taken over the Sikh temples, these groups. They [a small group of people who were trying to promote an independent State of Khalistan by violent means] would be threatening to you there. There were beatings in the community.[55]

Tara Singh Hayer's daughter-in-law, Isabelle Hayer (also Martinez-Hayer), told the Commission about the "extensive" terror that was felt in the Indo-Canadian community at that time.[56]

The Hon. Ujjal Dosanjh testified about the treatment of Indo-Canadians who publicly opposed Sikh extremism or who resisted demands to embrace extremism after the 1984 Golden Temple incident in Amritsar. He said that, beginning in 1984, Sikhs in Canada were "…left to fend for ourselves" when Canadian institutions were unable to deal with "…a wave of hatred, violence, threats, hit lists, silencing of broadcasters, journalists, activists."[57] He said that moderates who sought to regain control of Sikh temples in the 1990s were brutally beaten.[58]

---

52 *Lessons to be Learned: The report of the Honourable Bob Rae, Independent Advisor to the Minister of Public Safety and Emergency Preparedness, on outstanding questions with respect to the bombing of Air India Flight 182* (Ottawa: Air India Review Secretariat, 2005), p. 3 [*Lessons to be Learned*].

53 *Lessons to be Learned*, p. 3.

54 Testimony of Dave Hayer, vol. 76, November 15, 2007, pp. 9528-9529.

55 Testimony of Dave Hayer, vol. 76, November 15, 2007, pp. 9533-9534.

56 Testimony of Isabelle Martinez-Hayer, November 15, 2007, vol. 76, pp. 9534-9535.

57 Testimony of Ujjal Dosanjh, vol. 80, November 21, 2007, p. 10168.

58 Testimony of Ujjal Dosanjh, vol. 80, November 21, 2007, p. 10175.

Dosanjh's account of the intimidation that he, his family and others faced highlights the risks encountered by individuals who did not yield to intimidation:

> So there used to be hit lists and you would get anonymous letters delivered through your mail slot or by mail by some regiment or other organization that they were going to eliminate you and "reform you", and I was no exception. So I received some of those things as well.
>
> . . .
>
> There were threats to kidnap my children, and this was 1984-85, and my eldest son was 11 years old. I have three sons. And there were threats on the phone, message recorder threats to kill my children, kill my wife, abduct my children, firebomb my home, kill me and these came of course, as I said, directly sometimes on the phone, on the voice mail, through third parties, in fact.
>
> One time I remember a threat was directly given to a distant relative of mine that I would be killed that particular night. And that threat was then delivered, passed on to my brother-in-law who, en masse with his entire family, ended up at my home at 11 o'clock at night while I am sleeping on the mattress on the floor, on the ground floor worried about being firebombed with my children sleeping on the top floor. We slept on the ground floor, on the mattresses or even on the carpet floor for almost several years because we were worried somebody might firebomb our house and ... and we would all be going up in smoke if we were sleeping on the top floor.
>
> . . . One watched one's back all the time.[59]

Undoubtedly, intimidation to prevent individuals from speaking out against extremist agendas would foster a general atmosphere of fear that would also make community members reluctant to help authorities in terrorism investigations and prosecutions. Vancouver Police Department Detective Don McLean, who worked in the Sikh community as part of the Indo-Canadian Liaison Team before and immediately after the Air India bombing, indicated in testimony that the level of intimidation in the Vancouver Sikh community was comparable to that found in communities suffering intimidation from organized criminal groups and that there was a generalized fear of reprisals against those who cooperated with police.[60]

---

59 Testimony of Ujjal Dosanjh, vol. 80, November 21, 2007, pp. 10169-10172.
60 Testimony of Don McLean, vol. 35, May 29, 2007, pp. 4131-4132.

Dave Hayer referred to a perception among Indo-Canadians that organizations such as Babbar Khalsa are politically influential, and can operate with impunity. He testified that the Air India acquittals reinforced this impression, allowing intimidation in the Sikh community to increase.[61]

8.3.6 Reducing Intimidation and Promoting Trust

The authorities must understand the intimidation and threats that witnesses face and take the most appropriate measures to protect them. Dandurand suggested several ways to increase trust in the authorities and to avoid or limit the damage done by attempts to intimidate communities:

- hiring, training and promoting officers from a variety of cultural backgrounds, including "target" communities, to help build bridges with those communities and increase the level of confidence in the authorities;[62]
- providing training to all officers about the culture, language and customs of various communities;[63]
- receiving complaints about intimidation and providing a means for further contact should the intimidation become more serious;[64]
- thoroughly investigating complaints of intimidation, which may involve injecting the necessary resources;[65]
- following up with victims of intimidation and informing them, as well as the entire community, of the measures taken;[66]
- prosecuting incidents of intimidation to the full extent of the law to show criminals, as well the community, that such incidents are taken seriously;[67] and
- improving and developing the coordination of witness protection with foreign police forces.[68] Witness protection must be flexible enough to respond to the particular and often very difficult circumstances faced by witnesses in terrorism prosecutions.

---

61 Testimony of Dave Hayer, vol. 76, November 15, 2007, pp. 9539-9540, 9582.

62 Testimony of Yvon Dandurand, vol. 68, October 29, 2007, pp. 8570-8571. The idea of promoting officers implies hiring officers who are more than simple token police officers from a particular community. These officers would over time move up the chain of command.

63 Testimony of Yvon Dandurand, vol. 68, October 29, 2007, pp. 8571-8572.

64 Testimony of Yvon Dandurand, vol. 68, October 29, 2007, pp. 8577-8581. The Air India Victims' Families Association (AIVFA) also spoke of the need to give greater priority to investigating complaints of intimidation: "The authorities must respond vigorously to threats and not wait until actual acts of violence occur": *Where is Justice?* AIVFA Final Written Submission, Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, February 29, 2008, p. 174 [AIVFA Final Written Submission]. No other parties or intervenors commented on Professor Dandurand's findings and recommendations on this topic.

65 Testimony of Yvon Dandurand, vol. 68, October 29, 2007, p. 8579. See also Dandurand Paper on Protecting Witnesses, p. 76.

66 Testimony of Yvon Dandurand, vol. 68, October 29, 2007, p. 8580.

67 Testimony of Yvon Dandurand, vol. 68, October 29, 2007, p. 8579. See also Dandurand Paper on Protecting Witnesses, pp. 36, 77.

68 Testimony of Yvon Dandurand, vol. 68, October 29, 2007, pp. 8570-8591; vol. 69, October 30, 2007, pp. 8695-8698.

Honesty is essential. Authorities should not promise anonymity when it cannot be guaranteed – for example, when legal obligations, such as the right of an accused to disclosure of the identity of police agents, may well prevent promises from being honoured.

8.3.7 Witness Protection during the Air India Investigation

The preceding material described the intimidation of those who spoke against extremism or who were seen to be helping the authorities. In some cases, physical protection of these individuals was necessary. Yet the Commission's review of CSIS and RCMP dealings with witnesses and sources, and with each other, produced several examples of inadequate measures to protect witnesses.

Unlike CSIS, which viewed sources as "crown jewels," the RCMP often perceived them as informants or criminals who should be approached with skepticism and who should be expected to "put up or shut up." To the RCMP, the main value of sources was the evidence they could provide in a court of law as witnesses. The Force was relatively unconcerned with any value they could bring as confidential sources of intelligence.[69]

In several cases, the RCMP did an inadequate job in dealing with sources that CSIS had developed. The RCMP's aggressive all-or-nothing approach to Mr. A, for example, was indicative of its approach to sources as criminals and not as assets. It also showed the RCMP's insensitivity to the demands of potential witnesses for protection and other benefits.

The RCMP also failed to appreciate the need for successful partnership with the Sikh community for its investigations. In several cases, the RCMP showed a troubling lack of cultural sensitivity when approaching sources. Beyond the RCMP, the Government in general exhibited a wilful blindness to the intimidation and fear within the Canadian Sikh community.

The way in which the RCMP approached, treated and protected potential sources might have caused individual sources to refuse to provide further information. It may also have caused a greater wariness in the community about providing information to CSIS. CSIS investigator William Dean ("Willie") Laurie testified about this point:

> **MR. LAURIE:** … sometimes we were familiar with people who had been interviewed by the RCMP, ostensibly for the same purpose, and they were so intimidated that they could -- even if they wanted to help, they were convinced that they shouldn't help because they didn't want to be involved with people who treated them that way.
>
> **MR. KAPOOR:** Which way?

---

69 See Volume Two, Part 2, Post-Bombing, Chapter I, Human Sources: Approach to Sources and Witness Protection.

> **MR. LAURIE:** As though they had to participate, you know, that they were being forced into it, that they were being pushed under duress perhaps to assist because you must know something and we are the police after all, and you know, we can make trouble for you perhaps, or something like that. You know, we know somebody in your family who has had trouble with the law, blah, blah, blah, that sort of thing. It's not something that ever worked for people on my desk.[70]

The RCMP's failure to appreciate the ongoing threat posed by Sikh terrorism led the RCMP to approach at least one source in a manner which may have placed the source in danger. More generally, the RCMP had no strategies for dealing with fearful witnesses. In at least one instance, the RCMP repeatedly contacted a source to attempt to secure her cooperation without trying to meet her concerns.

Witness protection, in fact, was envisioned by the RCMP as a benefit to be provided to an individual in exchange for information and services. There was a perception that, until someone had "signed on" to help, it was premature for the RCMP to think about protection measures.

The following examples demonstrate a lack of sensitivity to witness protection issues during the Air India investigation and trial:

- The RCMP approached Mr. A, fully knowing that he did not wish to speak to the police. This approach caused Mr. A to express concern for his safety. RCMP members used an unmarked vehicle to visit Mr. A, but approached him publicly and unannounced, spoke to him on the doorstep of his residence in plain view of neighbours, and later required him to travel with them, all of which could have attracted unwanted attention from neighbours and others at his residence;[71]

- The RCMP's inadequate protection of Tara Singh Hayer may in large part be attributed to its inability to understand the larger context of the threats against him. By viewing such threats as localized and isolated incidents, the RCMP did not recognize the greater threat posed to Hayer by Sikh extremism. When RCMP members finally installed video cameras in Hayer's home, they failed to explain the proper functioning of the system to the family, installed the system in a less than optimal manner and did not monitor it adequately. After Hayer's murder, the RCMP discovered that the system

---

70 Testimony of William Laurie, vol. 61, October 15, 2007, pp. 7403-7404.
71 See Volume Two, Part 2, Post-Bombing, Section 1.1, Mr. A.

had failed to record any video of the shooting and did not disclose this failure to the family;[72]

- RCMP members failed to appreciate the threat that Bagri and his associates could pose to Ms. E's safety. Ms. E had a genuine fear for her safety and that of her family. Still, the RCMP continued to approach her in a public way, at times questioning her within earshot of others. RCMP members similarly made no serious attempt to assess the danger she faced by cooperating with police. In fact, the RCMP discounted Ms. E's fears in 1990. When the RCMP did ask her about her safety concerns, she was told to particularize and define her concerns herself and received no counselling or guidance to help her express her fears or understand the precautions that could be taken. Ms. E was also often approached in a confrontational and insensitive manner – for example, when RCMP officers repeatedly accused her of having had an affair with Bagri in spite of her denials and then told her common-law husband, who she was with at the time of the events, that she had been "seeing Bagri;"[73]

- CSIS "handed" Ms. D to the RCMP Air India Task Force after she provided information about Malik. The RCMP commercial crime section also dealt with Ms. D, since her information related in part to allegations of fraud. Ms. D's name was released when a warrant application was inadvertently left unsealed by the commercial crime section. Ms. D had to enter the RCMP Witness Protection Program much earlier than planned, which disrupted her life significantly.[74]

Conflicts between CSIS and the RCMP at times resulted in the loss of valuable sources and information. There was no collegial method of deciding when it was appropriate to "share" sources between the agencies. The eagerness of the RCMP to convert various sources into witnesses during the Air India investigation is understandable, given the magnitude of the crime. However, the RCMP was not as sensitive as it should have been when approaching those sources and not as effective as it should have been in providing for their safety.

8.3.8 Conclusion

Both community-wide intimidation and specific instances of intimidation played a role in the Air India investigations. The evidence before the Commission suggests that, even a quarter century after the Air India investigation began, intimidation is still very much an issue.

---

72 See Volume Two, Part 2, Post-Bombing, Section 1.2, Tara Singh Hayer.
73 See Volume Two, Part 2, Post-Bombing, Section 1.3, Ms. E.
74 See Volume Two, Part 2, Post-Bombing, Section 1.5, Ms. D.

Effective protection for threatened individuals and a firm response to incidents of intimidation bolster the credibility of the justice system. A pattern of threats without a police response simply strengthens the hand of extremists or terrorist groups. Even an isolated instance of ineffective protection or a single threatened or intimidated witness can seriously damage the credibility of the authorities and dissuade other members of the community from coming forward.

In terrorism investigations at least, the RCMP should not see witness protection as a benefit that must be earned by testimony. Reasonable steps should be taken to respond to a source's safety concerns even before the source is considered for formal admission to a witness protection program. The RCMP should become more familiar with problems of intimidation in the particular communities that may be involved in terrorism investigations. They should also recognize that not all witnesses in terrorism investigations will be criminals and that human sources can be a valuable source of intelligence about terrorism even if they do not testify in court.[75]

All authorities, including CSIS, must be honest in their dealings with sources. They must be careful to avoid making promises to sources which cannot be kept – for example, that the identity of a source will be kept confidential and that the source will never be required to testify. They must be candid about the burdens and the limits of witness protection programs. Deception breeds distrust among potential sources; distrust too often engenders their silence.

8.4 Protecting Identity to Avoid the Need for Witness Protection

The previous section explained some of the real dangers facing individuals whose assistance to intelligence and police agencies becomes known. In terrorism investigations and prosecutions, the surest way to protect individuals against direct intimidation is to ensure that their identity remains secret. If no prosecution occurs, keeping the identity of a source secret is relatively easy for skilled intelligence agents. However, there is a legitimate public interest in prosecuting many terrorism offences. Proceeding with a prosecution makes it much more difficult to protect the identity of those who help the authorities. Fortunately, the government and prosecutors do have an array of legal measures that can offer partial or total anonymity to sources and witnesses, reducing the chances that they will need to enter witness protection programs.

As discussed in Chapter IV, CSIS officials who testified before the Commission appeared to assume that preventing disclosure of identity was the main way to protect confidential sources.[76] CSIS officials should become fully aware of the legal system's many protections against disclosure, including informer privilege. Finally, CSIS should have access to programs to protect vulnerable witnesses and sources. These programs should facilitate continuity in the handling of sources to avoid the problems that arose in the Air India investigation when CSIS sources were transferrred to new and unfamiliar RCMP handlers.

---

75 See Volume Two, Part 2, Post-Bombing, Chapter I, Human Sources: Approach to Sources and Witness Protection.

76 See Section 4.5.

This section summarizes a variety of measures which can offer some protection to witnesses and sources when prosecutions proceed. As discussed in detail later, even the best-designed witness protection programs can pose significant hardships for those accepted into them. The preferred course of action is to look first for measures that avoid the need to enter witness protection. If these measures do not permit investigators to use information supplied by secret sources and allow prosecutors to satisfy their disclosure obligations, witness protection programs will be necessary.

8.4.1 The Role of Prosecutorial Discretion

One important safeguard in protecting sources and the safety of witnesses is the discretion of prosecutors to decide whether to commence or continue a prosecution. The Supreme Court of Canada has recognized that the Crown can properly use its power to stay or stop a prosecution as a means of protecting the identity of informers.[77]

Many terrorism offences in the *Criminal Code* attract lengthy maximum sentences. For example, instructing someone to carry out an activity for the benefit of a terrorist group,[78] instructing someone to carry out a terrorist act[79] and committing an indictable offence for the benefit of a terrorist group[80] all carry maximum sentences of life imprisonment.

Prosecutors may be tempted to proceed with as many terrorism charges as possible to increase the odds of conviction on some of them, but fewer, well-placed, charges could achieve the same result. The need to protect sources should be a factor that informs the exercise of prosecutorial discretion. This might reduce the number of individuals who would have their identities exposed to comply with disclosure obligations or to testify. In some cases, a non-terrorist criminal charge or perhaps a terrorist financing charge, as opposed to one based on an alleged terrorist plot, might protect sources who were privy to the details of the plot. As discussed in Chapter V, there are no disclosure obligations if the information is not relevant to the charges faced by the accused.[81]

However, prosecutorial discretion may be of limited utility in protecting sources because the courts may interpret disclosure obligations as applying to the entire investigation. Even a charge based on financing terrorism as opposed to charges that involve alleged terrorist plots will generally require disclosure in relation to issues such as the accused's intentions to facilitate or carry out a terrorist activity or to benefit a terrorist group.[82] The relevance of such issues could require wide-ranging disclosure. Such disclosure could place the identity of sources at risk.

---

77 *R. v. Scott*, [1990] 3 S.C.R. 979.
78 *Criminal Code*, R.S,C. 1985, c. C-46, s. 83.21 [*Criminal Code*].
79 *Criminal Code*, s. 83.22.
80 *Criminal Code*, s. 83.2.
81 *See R. v. Chaplin*, [1995] 1 S.C.R. 727.
82 *Criminal Code*, ss. 83.03, 83.04.

8.4.2 Editing Affidavits Prepared in Support of Applications for Warrants

As discussed in Chapter IV, the process for using electronic surveillance warrants obtained under section 21 of the *CSIS Act* or Part VI of the *Criminal Code* involves disclosing the affidavit used to obtain the warrant in the first place. Before disclosing the affidavit, the government can remove information that might reveal the identity of a confidential source. However, any identifying material deleted from the affidavit cannot be used to support the constitutionality of the warrant and the search. In some cases, withholding identifying information about a source could destroy the validity of the warrant. *R. v. Parmar*[83] is a case in point. There, an informant refused to allow his or her name to be disclosed. As a result, the prosecution did not disclose an affidavit that would reveal the informant's identity. The legality of the warrant could not be sustained without this information. Wiretap information obtained under an invalid warrant was, at that time, subject to automatic and absolute exclusion. The prosecution collapsed because of a failure to make full disclosure, which in turn stemmed from the informant's refusal to allow his or her name to be disclosed and to enter a witness protection program.

Chapter IV proposes a new regime that would allow security-cleared special advocates to represent the interests of the accused in challenging warrants under section 21 of the *CSIS Act* or Part VI of the *Criminal Code*. Special advocates would have complete access to the affidavit used to obtain the warrant, including information that identified any confidential source, and would represent the interests of the accused without disclosing the identity of the source to the accused. If adopted, this proposal could provide significant protections for informers while not sacrificing the ability to subject the warrant to adversarial challenge and to assert the accused's right to be secure against unreasonable search or seizure.

8.4.3 Relying on Police Informer Privilege

At common law, police informers (other than police agents and material witnesses) have a right to keep their identities from being revealed to the defence in a criminal prosecution. In *Named Person v. Vancouver Sun*, the Supreme Court of Canada described this "informer privilege" rule, noting that it "…protects from revelation in public or in court the identity of those who give information related to criminal matters in confidence."[84] The Court stressed that the duty to keep an informer's identity confidential applies to the police, the Crown, attorneys and judges, and that any information which might tend to identify an informer is protected by the privilege. The protection is not limited simply to the informer's name, but extends to any information that might lead to identification.[85]

---

83 (1987) 34 C.C.C. (3d) 260 (Ont. H.C.J.).
84 2007 SCC 43, [2007] 3 S.C.R. 252 at para. 16.
85 2007 SCC 43, [2007] 3 S.C.R. 252 at para. 26.

In an earlier Supreme Court decision, *R. v. Leipert*, then Justice McLachlin spoke of informer privilege as being of such importance that it cannot be balanced against other interests: "Once established, neither the police nor the court possesses discretion to abridge it."[86]

The police informer privilege rule is an exception to the broad right set out in *R. v. Stinchcombe*[87] for an accused to receive full disclosure. The privilege is absolute and allows an exception only where innocence is at stake. The innocence-at-stake exception arises if there is no way other than through disclosure for the accused to demonstrate innocence.[88] For example, the identity and evidence of an informer would have to be disclosed to the accused in cases where the informer had become a material witness or an *agent provocateur*.[89] Alternatively, the Crown could withdraw the charges against an accused to protect the identity of an informer.

At present, it is not clear whether police informer privilege applies to confidential CSIS sources. However, section 18 of the *CSIS Act* prohibits disclosure of confidential CSIS sources, albeit subject to many exceptions set out in section 18(2), including court-ordered disclosure. Chapter VI discusses the need for CSIS to be able to pass information to the RCMP without sacrificing the ability of informers or the state to claim informer privilege at a later date.

Chapter VI discusses how informers must be carefully managed. Both CSIS and the police should ensure that they have the most complete information possible before they promise anonymity to an informer in exchange for information. This care is required for a number of reasons. In some cases, the promise of anonymity may not be legally enforceable. For example, an officer might "suggest" that an informer ask specific questions to elicit certain information from the target of an investigation. Even years later at trial, a judge might decide that the individual was not an informer but became a police agent as a result of the police suggestion. The informer privilege would no longer apply.

In addition, promises of anonymity may seriously compromise the ability to commence a subsequent terrorism prosecution. As discussed earlier, the 1987 Hamilton prosecution of Talwinder Singh Parmar and others collapsed when an informer refused to consent to the disclosure of identifying information. In another case, charges for a 1986 conspiracy relating to a plot to blow up

---

86 *R. v. Leipert*, [1997] 1 S.C.R. 281 at para. 14. See also the discussion of informer privilege in Kent Roach, "The Unique Challenges of Terrorism Prosecutions: Towards a Workable Relation Between Intelligence and Evidence" in Vol. 4 of Research Studies: The Unique Challenges of Terrorism Prosecutions, pp. 66-67, 73-75 [Roach Paper on Terrorism Prosecutions].

87 [1991] 3 S.C.R. 326.

88 See Chapter VI. The *Witness Protection Program Act* contains a similar innocence-at-stake exception to the general obligation to protect information about the changed identity or location of an individual in a witness protection program. Section 11(3)(d) permits the RCMP Commissioner to disclose information about the location or a change of identity of a current or former "protectee" if the disclosure is essential to establish the innocence of a person in criminal proceedings.

89 *R. v. Scott*, [1990] 3 S.C.R. 979, discussed in Roach Paper on Terrorism Prosecutions, p. 167. At pages 157-165, Roach discusses the various judgments in *R. v. Khela* relating to a police informer, "Billy Joe," who had been promised anonymity.

another Air India aircraft were eventually stayed. The stay occurred, in large part, because a key informer had apparently been promised that his identity would never be revealed. The courts, however, found that the informer was not protected by informer privilege because he had acted as a police agent. The police remained reluctant to disclose information relating to the informer, and the case was eventually permanently stayed by the courts as a result.[90]

In some cases, the benefits of keeping a source's identity secret to obtain information which may prevent an act of terrorism can clearly outweigh the value of the source as a witness in a subsequent prosecution. Prevention may often be more important than prosecution. Difficult decisions by security intelligence and police officers to offer anonymity in exchange for information which may be urgently needed should not be second-guessed.

Both police and the Crown have developed policies to help ensure that informers do not lose their privileged status through state action.[91] These policies need to be extended and adapted for CSIS. Moreover, there needs to be greater coordination among the agencies involved in terrorism cases concerning the treatment of sources. The proposed Director of Terrorism Prosecutions discussed in Chapter III would be able to provide consistent and expert legal advice about the legal status of informers as they transferred from CSIS to the RCMP and, in some cases, back again. Each agency needs to better appreciate the needs and perspective of the other. Disputes about the ultimate use of human sources could, when necessary, be resolved through the intervention of the National Security Advisor, as described in Chapter II.

The law surrounding police informer privilege is complex and evolving. There may be considerable uncertainty in a particular terrorism investigation about whether a source is protected by privilege. In particular, questions may arise about when and whether valid promises of anonymity may have been made to the source, and whether a source who is otherwise protected by the privilege has lost that privilege by becoming an active agent, material witness or *agent provocateur*. The prudent path with such factual and legal uncertainty is to take reasonable steps to protect informers who are vulnerable to retaliation if identified publicly. At the same time the state, on behalf of the informer, should assert the police informer privilege to withhold identifying information.

---

90 *R. v. Khela* (1991), 68 C.C.C. (3d) 81 (Que. C.A.); *R. v. Khela*, [1995] 4 S.C.R. 201; *R. v. Khela* (1998), 126 C.C.C. (3d) 341 (Que. C.A.).

91 For example, the RCMP offers a one-week course entitled "Human Source Management" to train officers in the handling of agents and informers. One objective of the course is "…to ensure that an informer remains an informer and does not drift over into an agent capacity": Testimony of Raf Souccar, vol. 70, October 31, 2007, p. 8890. The Federal Prosecution Service Deskbook calls upon Crown counsel to obtain a full understanding of the nature of the relationship between the police and the informer/agent early on to determine the person's status and foresee any potential risks: Department of Justice Canada, The Federal Prosecution Service Deskbook, c. 36, online: Department of Justice Canada <http://www.justice.gc.ca/eng/dept-min/pub/fps-sfp/fpd/ch36.html> (accessed June 2, 2009).

8.4.4 Disclosure: Non-relevance and Timing

Stinchcombe imposes a broad constitutional duty on the state to retain and disclose relevant information to the accused. Prosecutors may properly refuse to disclose information, including information about identity, if the information is not relevant. Prosecutors may also refuse to disclose evidence that is subject to a valid privilege such as the police informer privilege.

Prosecutors also have a reviewable discretion about *when* they disclose evidence and could use this discretion to delay disclosing the identity of an informer or witness for his or her protection. Late disclosure can undermine the efficiency of a trial because it may lead to adjournments allowing the defence to review the disclosed material. Late disclosure might also reduce the chances of resolving a case before trial. For these reasons, prosecutors should not lightly decide to delay the disclosure of relevant information. Nevertheless, the need to protect the safety of informers and witnesses is one of the few reasons that will justify delayed disclosure. The delay in disclosure should, however, be limited to the time necessary to ensure effective protection for the individual whose safety may be jeopardized by the disclosure.

8.4.5 Sections 37 and 38 of the *Canada Evidence Act*

Section 37 of the *Canada Evidence Act* permits ministers to object to the disclosure of information by certifying that the information should not be disclosed on the grounds of a specified public interest. As discussed more fully in Chapter VII, the protection of informers is considered one of those public interests. The trial judge is permitted to balance the competing interests in disclosure and non-disclosure, and can make an order placing conditions on disclosure.[92] Thus, the judge might prohibit disclosing the identity of an informer. At the same time, the judge can make an order to protect the right of the accused to a fair trial. This could include a stay of proceedings.[93]

Section 38 of the *Canada Evidence Act* allows the Attorney General of Canada to seek non-disclosure orders on the basis that the disclosure of information would harm national security, national defence or international relations. Similar to section 37, the judge is allowed to balance competing interests in disclosure and non-disclosure and place conditions on disclosure. As a result, the judge might prohibit disclosing the identity of an informer. Section 38 might be of particular importance to prevent harm to national security that would flow from a successful argument that the transfer of human sources from CSIS to the RCMP resulted in a loss of informer privilege.

Chapter VII recommends how to improve the efficiency and fairness of the process used to obtain judicial non-disclosure orders under section 38. In appropriate cases, sections 37 and 38 could be used to prevent the disclosure of identifying information about an informer. The public interest or Crown privileges asserted under these sections provide less protection than the privilege for police informers.

---

92 *Canada Evidence Act*, R.S.C. 1985, c. C-5, s. 37(5) [*Canada Evidence Act*].
93 *Canada Evidence Act*, s. 37.3.

8.4.6 "Partial Anonymity"

The measures discussed above all relate to the pre-trial stages of a prosecution and involve attempts to prevent the disclosure of identifying information about informers to the accused. Several measures are also available to offer some protection to witnesses at the actual trial, either by limiting access to information about their identities (for example, through publication bans) or by permitting measures to make them feel less intimidated when they testify.

Many of these partial anonymity measures will only protect the witness against intimidation by those other than the accused because, in most cases, the accused will already know the identity of the witness. It may be possible in some cases to allow a witness, particularly an undercover officer, to testify using a pseudonym. In this way, the accused does not learn the actual identity of the witness even though the Crown has disclosed all relevant information about the witness to the accused. The issue of anonymous testimony, where the accused does not know the identity of the witness, is examined in the next section.

Partial anonymity measures constitute exceptions to the "open court principle" recently articulated by Justice Lebel in *Named Person v. Vancouver Sun*:

> In general terms, the open court principle implies that justice must be done in public. Accordingly, legal proceedings are generally open to the public. The hearing rooms where the parties present their arguments to the court must be open to the public, which must have access to pleadings, evidence and court decisions.[94]
>
> . . .
>
> The open court principle is not absolute, however. A court generally has the power, in appropriate circumstances, to limit the openness of its proceedings by ordering publication bans, sealing documents, or holding hearings *in camera*. It can also authorize an individual to make submissions or appear in court under a pseudonym should this be necessary in the circumstances. In some cases, courts may be required by statute to order such measures. In others, they are merely authorized to do so, whether under legislation granting them this power or — where superior courts are concerned — pursuant to their inherent power to control their own processes.[95]

Many of these exceptions to the open court principle are found in the *Criminal Code*:

---

94 2007 SCC 43, [2007] 3 S.C.R. 253 at para. 81.
95 2007 SCC 43, [2007] 3 S.C.R. 253 at para. 91.

- **Excluding the public from the courtroom**: Section 486(1) allows a judge to exclude members of the public from the courtroom for all or part of the proceedings in the interest of the proper administration of justice. This includes ensuring that justice system participants (which would include witnesses) are protected.[96]

- **Testifying outside the courtroom, etc.**: If an accused is charged with a terrorism offence set out in the *Criminal Code*, the judge may order that some or all witnesses testify outside the courtroom if the order is necessary to protect the safety of the witnesses. The judge may order that a witness testify behind a screen or similar means of preventing the witness from seeing the accused if the judge concludes that the order is necessary to obtain a full and candid account from the witness.[97]

  A witness can, however, testify outside the courtroom only if the accused, the judge and the jury can watch the testimony by closed-circuit television or otherwise and the accused is permitted to communicate with counsel while watching the testimony.[98] The accused can still see the witness, but the witness has the comfort of not having to see the accused while testifying.

A 2006 Australian federal criminal case, *R. v. Lodhi*,[99] suggests how partial anonymity measures might be further expanded in Canada. In pre-trial proceedings, the judge ordered that a screen be used so that the accused could not identify Australian Security Intelligence Organisation (ASIO) officers when they testified. This was to prevent "…the real possibility of the compromise of intelligence operations in Sydney."[100] The parties consented to the ASIO officers testifying via closed-circuit television at the trial, instead of using screens. Monitors were available to all court participants, including the accused. However, the accused's monitor was intentionally not operational, though the jury apparently did not know this.[101]

- **Publication bans**: Section 486.5(1) of the *Criminal Code* allows a judge to make an order directing that any information that could identify a witness not be published, broadcast or

---

96 R.S.C. 1985, c. C-46, s. 486(2)(b). Section 2 of the *Criminal Code* defines "justice system participant" to include "an informant, a prospective witness, a witness under subpoena and a witness who has testified."

97 *Criminal Code*, s. 486.2(4). In upholding a previous version of this section under the *Charter*, the Supreme Court noted that the accused could still see the complainant and the screen would not adversely affect the accused's right to cross-examine the witness: *R. v. Levogiannis*, [1993] 4 S.C.R. 475.

98 *Criminal Code*, s. 486.2(7).

99 [2006] NSWSC 596.

100 [2006] NSWSC 596 at para. 59.

101 See the more extensive discussion of the *Lodhi* case in Roach Paper on Terrorism Prosecutions, pp. 282-286.

transmitted if the judge is satisfied that the order is necessary for the proper administration of justice. In deciding whether to make an order, the judge must consider several factors that relate to the well-being of the witness:

- whether there is a real and substantial risk that the witness would suffer significant harm if his or her identity were disclosed;
- whether the witness needs the order for their security or to protect him or her from intimidation or retaliation; and
- whether effective alternatives are available to protect the identity of the witness.[102]

- **Pseudonyms**: As Justice Lebel noted in *Named Person v. Vancouver Sun*, a court can authorize an individual to make submissions or appear in court under a pseudonym if necessary in the circumstances.[103] Testifying under a pseudonym is another vehicle for shielding the identity of a witness from the general public. It might also prevent the accused from learning the true identity of the witness – for example, if the accused only knew the witness under that person's assumed name. However, a pseudonym would offer little protection to a witness if the witness could be identified by the accused even while testifying under a pseudonym. Still, pseudonyms may be especially important and valuable in protecting the identity of CSIS officers and undercover officers who may be required to testify in terrorism prosecutions.

These various measures seek to provide "partial anonymity" and offer some, but not total, identity protection to witnesses at trial. The accused can still determine the identity of the witness if the witness testifies by closed-circuit television or behind a screen, as well as when there is a publication ban or order removing the public from the courtroom. Even testifying using a pseudonym does not guarantee anonymity, since the accused can see the witness.

8.4.7 Conclusion

This section has considered various ways to protect the identity of individuals necessary for the proper prosecution of a trial and at the same time avoid the need to have them enter a witness protection program. As well, this section has discussed the important role of police informer privilege and judicial non-disclosure orders under sections 37 and 38 of the *Canada Evidence Act* in preventing the disclosure of identifying information about an informer. However, the privilege and these measures may impair terrorism prosecutions, in part because the informer will not be available to testify in such cases.

---

102 *Criminal Code*, s. 486.5(7).
103 2007 SCC 43, [2007] 3 S.C.R. 252 at para. 91.

Several other options offer a middle ground between protecting informers through anonymity and completely disclosing their identity. These options include delayed disclosure to allow sufficient time to put protection measures in place, the exercise of prosecutorial discretion about laying charges and the commencement and continuation of prosecutions, as well as the use of a variety of "partial anonymity" devices that limit the disclosure of the identity of a witness to the public.

The real dangers faced by some witnesses and their families makes it imperative that judges and prosecutors carry out their functions within a "culture of security." They must understand the risks to witnesses and sources and the variety of measures that can protect them, while still providing a fair trial to an accused. Dean Anne-Marie Boisvert of the Faculty of Law, l'Université de Montréal, spoke about this culture of security before the Commission:

> I think that we will have to develop an awareness and a culture of security, while preserving, of course, the fundamental rights of our Justice system.… Crown prosecutors have, on occasion, been too timid in their objections to disclosure applications; the judiciary has also, on occasion, been timid or could have ordered disclosure subject to certain conditions.[104] [translation]

As a general rule, whenever an individual's identity may need to be revealed to further a prosecution, the preferred option should be to reveal only as much identifying information as is necessary to ensure the viability of the prosecution and fairness to the accused. If a partial anonymity measure satisfies the needs of the prosecution and ensures fairness for the accused, the prosecution should not resort to a procedure that may fully expose the witness and possibly force him or her into a highly restrictive witness protection program.

Although they can be important, partial anonymity measures only go so far. They still contemplate that the accused and perhaps others will learn the identity of the witness. The next section examines the option of anonymous testimony in which even the accused does not know the identity of the witness.

8.5 Anonymous Testimony

As discussed earlier, the *Criminal Code* provides several measures that offer "partial anonymity" by allowing a witness to testify at a remote location, or while protected by a publication ban, closed court or physical screen. These measures may reduce the threat and discomfort that witnesses feel when they testify. Nevertheless, none of these measures would prevent a determined person from learning the identity of a witness.[105]

---

104 Testimony of Anne-Marie Boisvert, vol. 69, October 30, 2007, pp. 8771-8773.

105 Jean-Paul Brodeur, "The Royal Canadian Mounted Police and the Canadian Security Intelligence Service: A Comparison of Occupational and Organizational Cultures" in Vol. 1 of Research Studies: Threat Assessment RCMP/CSIS Co-operation, p. 204.

The limits of partial anonymity measures raise the question of whether witnesses facing serious threats in terrorism prosecutions should be permitted to testify in complete anonymity. Since their identities would remain secret, they would not need to consider enduring the hardship of a witness protection program. Although Canada does not at present allow anonymous testimony, some other democracies do.

There is no statutory authority in Canada for anonymous testimony. Section 650 of the *Criminal Code* requires the accused to be present at trial when evidence is given. This provision has been interpreted broadly by the Supreme Court of Canada to include all proceedings where the accused's interests are at stake.[106]

In the landmark disclosure case of *R. v. Stinchcombe*,[107] Justice Sopinka recognized that while informer privilege could protect the identity of some informers, "…it is a harsh reality of justice that ultimately any person with relevant evidence must appear to testify," adding that witnesses "…will have to have their identity disclosed sooner or later." Anonymous testimony runs contrary to judicial trends that favour extensive disclosure to the accused,[108] including disclosure of information about potential witnesses. This information can be useful to the accused in challenging the credibility of statements made by a witness.

Professor Dandurand observed that many European countries allow anonymity for those who provide evidence in criminal proceedings, but only in exceptional circumstances and in compliance with European human rights law.[109] Belgium, France, Germany, The Netherlands, Moldova, Finland[110] and now, most recently, the United Kingdom have all enacted rules allowing anonymous testimony under tightly controlled circumstances. In each case, the rules conform to the three guiding principles set by the European Court of Human Rights:

- There must be compelling reasons to justify anonymity;
- The resulting limitations on the effective exercise of the rights of the defence must have been adequately compensated for; and
- The conviction must not be exclusively or substantially based on anonymous testimony.[111]

Dandurand described in general the restrictions on anonymous testimony in jurisdictions where it is permitted:

---

106 *R. v. Vezina*, [1986] 1 S.C.R. 2; *R. v. Barrow* [1987] 2 S.C.R. 694.
107 [1991] 3 S.C.R. 326 at 339, 335.
108 See, for example, *Charkaoui v. Canada (Citizenship and Immigration)*, 2008 SCC 38, [2008] 2 S.C.R. 326 and *R. v. Stinchcombe*, [1991] 3 S.C.R. 326.
109 Dandurand Paper on Protecting Witnesses, p. 54.
110 Dandurand Paper on Protecting Witnesses, p. 55, citing N. Piancete, "Analytical Report" in Council of Europe, *Terrorism: Protection of Witnesses and Collaborators of Justice* (Strasbourg: Council of Europe, 2006), p. 19.
111 Dandurand Paper on Protecting Witnesses, p. 55.

- It is generally limited to cases where there is reason to believe that the witness would be seriously endangered;
- The decision to grant the status of anonymous witness rests with the *juge d'instruction*, who must interview the witness, who will be under oath;
- The principal elements to be established during the interview are the risk to the witness, and the identity, credibility, and reliability of the witness;
- The accused, accused's counsel, and the public prosecutor can be excluded from the interview, although the public prosecutor may follow the interview through an audio-link with a voice transformer or other secure means;
- The defence may be allowed to follow the interview and ask questions via audio link, but may also be limited to submitting a list of questions to the judge beforehand;
- If, after weighing the interests of the defence against those of the witness, the judge is satisfied that anonymity should be allowed, the Crown will be allowed to use statements of that witness as evidence in court. However, a conviction may not be based on these statements alone; and
- It is also often possible to grant partial anonymity to witnesses at risk.[112]

Even where anonymous testimony is allowed in Europe, it has caused controversy and is rarely used.[113] Dandurand explained some of the reasons for the controversy:

> There are significant issues surrounding the legitimacy and legality of the use of such measures and, in the words of one vocal critic of this approach: "Arguments in favour of witness anonymity are based on the contention that prejudice to the accused can be minimized and that which remains can be justified through a purported "balancing" of competing interests in the administration of justice. The problem with this approach, despite its superficial appeal, is that it is unfairly balanced against the accused from the very outset."[114]

---

112 Dandurand Paper on Protecting Witnesses, pp. 53-55.

113 For example, The International Criminal Defence Attorneys' Association, in its submission to the United Nations Preparatory Conference on the International Criminal Court Rules of Procedure and Evidence, opposed anonymous testimony, arguing that complete witness anonymity is only appropriate in instances where the individual is an informant who aided in the discovery of admissible evidence, but is not testifying against the accused in the proceeding: International Criminal Defence Attorneys Association, *Protection of Witnesses*, Position Paper presented during the United Nations Preparatory Conference on ICC Rules of Procedure and Evidence, 26 July - 13 August 1999, July 15, 1999, p. 3. See also Dandurand Paper on Protecting Witnesses pp. 54-55.

114 Dandurand Paper on Protecting Witnesses, p. 55.

Dandurand also noted the limited value of anonymous testimony:

> Even when permitted by law, the procedure for granting partial or full anonymity to a witness tends to be rarely used because of how, in practice, it can limit the admissibility of various elements of their testimony.[115]

Allowing anonymous testimony would also necessarily mean not revealing identity during disclosure.

8.5.1 The British Experience with Anonymous Testimony

In *R. v. Davis*,[116] the House of Lords overturned a murder conviction after three witnesses who identified the accused as the gunman testified under pseudonyms because they feared for their lives. The accused alleged that his ex-girlfriend was behind a plot to falsely accuse him of the murder, but he was not allowed to ask the witnesses any questions that would reveal their identity. The anonymous testimony was decisive in the accused's conviction, and Lord Brown concluded that "…effective cross-examination in the present case depended upon investigating the potential motives for the three witnesses giving what the defence maintained was a lying and presumably conspiratorial account."[117]

The House of Lords stressed that the ability of the accused to confront and cross-examine known witnesses had long been fundamental to the common law. It noted that some departures had been made long ago in the national security context including, for example, the treason trial of Sir Walter Raleigh, but that these departures were much criticized.[118] The use of anonymous witnesses had been proposed but rejected even in Northern Ireland during the height of concerns about the intimidation of witnesses and other justice system participants.[119]

The House of Lords relied on authority under the *European Convention on Human Rights*[120] that holds that no conviction should be based solely or to a decisive extent on anonymous testimony.[121] The focus of this jurisprudence is not on the admissibility of evidence under national law, but on "…whether the proceedings as a whole, including the way in which evidence was taken, were

---

115 Dandurand Paper on Protecting Witnesses, p. 54.
116 [2008] UKHL 36.
117 [2008] UKHL 36 at para. 96.
118 [2008] UKHL 36 at para. 5.
119 [2008] UKHL 36 at para. 6. Some anonymous testimony was used in a trial in Belfast for murder of two members of the British army, but no objection was made by the defence and the evidence did not implicate the accused in the killings and the credibility of the anonymous witnesses (press photographers) was not at issue: [2008] UKHL 36 at paras. 12, 53 and 73, discussing *R. v. Murphy* [1990] NI 306.
120 Section 6(3)(d) of the *European Convention on Human Rights* provides that everyone charged with an offence has "…the right to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him."
121 [2008] UKHL 36 at para. 25.

fair."[122] It is also significant that the European case law to date is grounded in an "inquisitorial" context where the judge not only knows the identity of the witness, but also has a mandate to investigate the case.[123]

A little more than a month after the decision in *R. v. Davis*, the United Kingdom enacted the *Criminal Evidence (Witness Anonymity) Act 2008*.[124] The Act abolished "…the common law rules relating to the power of a court to make an order for securing that the identity of a witness in criminal proceedings is withheld from the defendant."[125] The Act potentially applies in all criminal cases. Its provisions will expire at the end of 2009 unless extended for a 12-month period by the Secretary of State.[126]

The Act allows both the prosecutor and the accused to apply to a court for an anonymity order as well as a range of other measures, such as the use of pseudonyms and screens to prevent the disclosure of identifying information.[127] Although both the accused and the prosecutor can apply for such measures, there are specific measures for *ex parte* hearings in the absence of a defendant if the court concludes that they are appropriate.[128] The Act is silent on the appointment of special human rights advocates.

Under the Act, a court must be satisfied that three conditions, described as conditions A to C, are met before it can make an anonymity order. The conditions are as follows:

> Condition A is that the measures to be specified in the order are necessary
>
> > (a) in order to protect the safety of the witness or another person or to prevent any serious damage to property, or
> >
> > (b) in order to prevent real harm to the public interest (whether affecting the carrying on of any activities in the public interest or the safety of a person involved in carrying on such activities, or otherwise).
>
> Condition B is that, having regard to all the circumstances, the taking of those measures would be consistent with the defendant receiving a fair trial.

---

122 *Doorson v. Netherlands* (1996) 22 EHRR 330 at para. 67.
123 *Doorson v. Netherlands* (1996) 22 EHRR 330 at para. 73.
124 (U.K.), 2008, c. 15.
125 *Criminal Evidence (Witness Anonymity) Act 2008* (U.K.), 2008, c. 15, s. 1(2) [U.K. *Criminal Evidence (Witness Anonymity) Act 2008*].
126 U.K. *Criminal Evidence (Witness Anonymity) Act 2008*, s. 14.
127 U.K. *Criminal Evidence (Witness Anonymity) Act 2008*, ss. 2-3.
128 U.K. *Criminal Evidence (Witness Anonymity) Act 2008*, s. 3(7).

> Condition C is that it is necessary to make the order in the interests of justice by reason of the fact that it appears to the court that
>
> (a) it is important that the witness should testify, and
>
> (b) the witness would not testify if the order were not made.[129]

Condition A would be satisfied where there are concerns about the safety of the witness. The Crown Prosecution Service, in its guidelines for prosecutors, has interpreted safety concerns to relate both to specific threats to a witness as well as "…a general climate of fear in the environment in which the witness lives." In either case, it is essential that the Crown Prosecutor be satisfied that the police have evidence to support the concerns of the witness.[130] Condition A also covers a broad range of public interests. It can allow for police officers and other officials to give anonymous testimony.

Condition C relates to concerns that important witnesses might not testify if not protected by an anonymity order.

In many cases, the most difficult determination under the new legislation will be Condition B, which requires that the anonymity order be consistent with the defendant receiving a fair trial. The court can consider all relevant circumstances, but section 5(2) of the Act specifies that consideration should be given to the following factors:

> (a) the general right of a defendant in criminal proceedings to know the identity of a witness in the proceedings;
>
> (b) the extent to which the credibility of the witness concerned would be a relevant factor when the weight of his or her evidence comes to be assessed;
>
> (c) whether evidence given by the witness might be the sole or decisive evidence implicating the defendant;
>
> (d) whether the witness's evidence could be properly tested (whether on grounds of credibility or otherwise) without his or her identity being disclosed;
>
> (e) whether there is any reason to believe that the witness

---

129 U.K. *Criminal Evidence (Witness Anonymity) Act 2008*, s. 4.

130 Crown Prosecution Service (United Kingdom), "The Director's Guidance on Witness Anonymity", online: Crown Prosecution Service (United Kingdom) <http://www.cps.gov.uk/publications/directors_guidance/witness_anonymity.html#04> (accessed June 2, 2009).

> (i) has a tendency to be dishonest, or
>
> (ii) has any motive to be dishonest in the circumstances of the case,
>
> having regard (in particular) to any previous convictions of the witness and to any relationship between the witness and the defendant or any associates of the defendant;
>
> (f) whether it would be reasonably practicable to protect the witness's identity by any means other than by making a witness anonymity order specifying the measures that are under consideration by the court.

These provisions recognize that accused persons have a traditional right to know the identity of witnesses who testify against them. They also recognize that an anonymity order may make it difficult for an accused to test the credibility of the witness, including credibility in matters such as the relationship of the witness with the accused.

In response to the European Convention on Human Rights, the legislation instructs judges to consider whether the anonymous evidence will be "the sole or decisive evidence" against the accused. As noted above, under the European Convention, no conviction should be based solely or to a decisive extent on anonymous testimony.

The British legislation also addresses the need for proportionality by requiring the judge to consider whether "it would be reasonably practicable to protect the witness's identity" by less drastic means. This refers to partial anonymity devices discussed above, such as the use of remote testimony, screens or publication restrictions.

8.5.2 Anonymous Testimony and the Adversarial System

The British experience, as well as related experience in New Zealand,[131] demonstrates that anonymous testimony can be used in common law countries. Nevertheless, anonymous testimony has been used mostly in civil law jurisdictions where the judge (who knows the identity of the witness) can play an active investigative role.

In *Charkaoui v. Canada (Citizenship and Immigration)*, Chief Justice McLachlin highlighted a fundamental distinction between inquisitorial and adversarial systems:

---

131 New Zealand *Evidence Act 2006*, ss. 110-120. These provisions allow for anonymity orders both for preliminary hearings and trials and also contemplate the appointment of independent counsel to assist the judge.

> In inquisitorial systems, as in Continental Europe, the judge takes charge of the gathering of evidence in an independent and impartial way. By contrast, an adversarial system, which is the norm in Canada, relies on the parties — who are entitled to disclosure of the case to meet, and to full participation in open proceedings — to produce the relevant evidence. The designated judge under the [*Immigration and Refugee Protection Act*] does not possess the full and independent powers to gather evidence that exist in the inquisitorial process. At the same time, the named person is not given the disclosure and the right to participate in the proceedings that characterize the adversarial process. The result is a concern that the designated judge, despite his or her best efforts to get all the relevant evidence, may be obliged — perhaps unknowingly — to make the required decision based on only part of the relevant evidence.[132]

The Chief Justice noted that the role assigned to judges under the *Immigration and Refugee Protection Act*[133] was "*pseudo*-inquisitorial." She stated that "…[t]he judge is not afforded the power to independently investigate all relevant facts that true inquisitorial judges enjoy. At the same time, since the named person is not given a full picture of the case to meet, the judge cannot rely on the parties to present missing evidence. The result is that, at the end of the day, one cannot be sure that the judge has been exposed to the whole factual picture."[134] These comments underline some of the difficulties and dangers of using anonymous testimony in a common law adversarial system.

There was no consensus among parties and intervenors before the Commission about allowing anonymous testimony. There was some support for such testimony, but also a recognition of the legal problems that it might cause.[135]

8.5.3 Anonymous Testimony and the *Charter*

Any provision allowing for anonymous testimony would be challenged as infringing the accused's rights under sections 7 and 11(d) of the *Charter*. The first question would be whether the right to know the identity of a witness in

---

132 2007 SCC 9, [2007] 1 S.C.R. 350 at para. 50.

133 S.C. 2001, c. 27.

134 2007 SCC 9, [2007] 1 S.C.R. 350 at para. 51.

135 B'nai Brith supported importing anonymous testimony for "innocent bystander witnesses" into Canadian law: Final Submissions of the Intervenor, B'nai Brith Canada, paras. 86-87. The AIVFA acknowledged that the use of anonymous witnesses involves a number of complex procedural and substantive issues, and called for further investigation and consideration of the issue: AIVFA Final Written Submission, p. 173. The Criminal Lawyers' Association argued that "…witness anonymity will always detract from the accused's ability to full test the credibility of that witness" but also suggested that anonymous testimony would be better than reliance on hearsay or an inability to call a witness for the defence: Submissions of the Criminal Lawyers' Association, February 2008, pp. 45-46. The Attorney General of Canada did not comment on allowing anonymous testimony, but suggested that the Commission consider cautiously Dandurand's recommendations, stating that "…further analysis is necessary to determine whether they are applicable to or compatible with the Canadian legal framework": Final Submissions of the Attorney General of Canada, Vol. III, February 29, 2008, para. 198 [Final Submissions of the Attorney General of Canada].

order to challenge that person's evidence is a principle of fundamental justice under section 7 and/or a requirement of a fair trial under section 11(d).

If the accused's rights were violated by anonymous testimony, the second question would be whether and in what circumstances the violation could be justified under section 1 of the *Charter*.

8.5.3.1 No Right to Physical Confrontation of a Witness but a Right to Have an Opportunity to Engage in Cross-Examination

In the 1989 case of *R. v. Potvin*,[136] the Supreme Court of Canada upheld a provision that allowed evidence given by a witness at a preliminary inquiry to be used at trial when the witness was not available. The accused argued that his "…ability to cross-examine all adverse witnesses at trial before the trier of fact is a principle of fundamental justice and a requirement of a fair trial. Basic to this argument is an acceptance of the proposition that the trier of fact will be unable to assess the credibility of a witness in the absence of his or her physical presence at the time the evidence is presented to the trier of fact."[137] The Court held that such a proposition did not qualify as a principle of fundamental justice under section 7 of the *Charter* because, "…[o]ur justice system has…traditionally held evidence given under oath at a previous proceeding to be admissible at a criminal trial if the witness was unavailable at the trial for a reason such as death, provided the accused had an opportunity to cross-examine the witness when the evidence was originally given."[138] These authorities "…indicate that the right to confront unavailable witnesses at trial is neither an established nor a basic principle of fundamental justice."[139]

Although the Court decided that the right to confront witnesses was not a principle of fundamental justice, it did hold that the accused's opportunity to have cross-examined the witness at an earlier point at the preliminary inquiry was a constitutional requirement.[140] In the case of anonymous testimony, the question would be whether the inability to learn the identity of the witness would so damage the accused's cross-examination on issues of credibility that the accused could not be said to have had an opportunity to cross-examine the witness, as section 7 of the *Charter* requires.

8.5.3.2 Anonymous Testimony and the Right of Cross-Examination

The hearsay rule generally prohibits the introduction of a statement when the declarant is not available to be cross-examined by the accused. Exceptions to the hearsay rule can produce situations where an accused may not be able to cross-examine the person who makes a statement against him that has been given in evidence. Exceptions must be justified on the basis of necessity and reliability.[141] Justice Binnie observed that "…while in this country an accused

136 [1989] 1 S.C.R. 525.
137 [1989] 1 S.C.R. 525 at 540.
138 [1989] 1 S.C.R. 525 at 540.
139 [1989] 1 S.C.R. 525 at 542-543.
140 [1989] 1 S.C.R. 525 at 544.
141 *R. v. Starr*, 2000 SCC 40, [2000] 2 S.C.R. 144.

does not have an absolute right to confront his or her accuser in the course of a criminal trial, the right to full answer and defence generally produces this result."[142] Reliability is a particular concern with exceptions to the hearsay rule, since the accused may not be able to cross-examine the person who made the hearsay statement.

Anonymous testimony makes it difficult for the accused to cross-examine a witness effectively without knowing the identity of the witness. The South African Constitutional Court rejected anonymous testimony on the basis that it "has far more drastic consequences" than the use of publication bans and *in camera* hearings or screens. It noted that depriving the accused of the identity of the witness would mean the following:

> No investigation could be conducted by the accused's legal representatives into the witness's background to ascertain whether he has a general reputation for untruthfulness, whether he has made previous inconsistent statements nor to investigate other matters which might be relevant to his credibility in general.
>
> It would make it more difficult to make enquiries to establish that the witness was not at places on the occasions mentioned by him.
>
> It would further heighten the witness's sense of impregnability and increase the temptation to falsify or exaggerate….[143]

The United States Supreme Court reached a similar conclusion:

> The witness' name and address opens countless avenues of in-court examination and out-of-court investigation. To forbid this most rudimentary inquiry at the threshold is effectively to emasculate the right of cross-examination itself.[144]

Thus, the main problem with anonymous testimony lies in its impairment of the accused's ability to engage in full and informed cross-examination. Cross-examination has long been regarded as the best means of achieving the truth. Some wrongful convictions in Canada have been directly related to the inability of the accused to conduct a full and informed cross-examination of a lying witness.[145]

142 *R. v. Parrott*, 2001 SCC 3, [2001] 1 S.C.R. 178 at para. 51.
143 *S v. Leepile* 1986 (4) S.A. 187 at 189.
144 *Smith v. Illinois* 390 U.S. 129 at 130 (1967).
145 The Royal Commission on the Donald Marshall, Jr., Prosecution concluded that "We believe a full and complete cross-examination of John Pratico at this stage by [Marshall's lawyer] almost certainly would have resulted in his recanting the evidence given during his examination-in-chief that he had seen Marshall stab Seale. In those circumstances, no jury would have convicted Donald Marshall, Jr.": *Royal Commission on the Donald Marshall, Jr., Prosecution*, vol. 1 - Findings and Recommendations (Halifax: Royal Commission on the Donald Marshall, Jr., Prosecution, 1989), p. 79.

8.5.3.3 Section 7 of the Charter and Anonymous Witnesses

Anonymous testimony might be held to violate fair trial rights under section 7 of the *Charter*, including the accused's right to know the case to meet, the accused's right to make full answer and defence and the accused's right to conduct a full cross-examination. The right to confront a known witness at some point in the trial process might also be held to be a principle of fundamental justice in its own right. This would not necessarily be inconsistent with the ruling in *Potvin* that the actual confrontation between the accused and an unavailable witness at trial is not a principle of fundamental justice, as long as the accused has had a previous opportunity to cross-examine the witness.

The accused's right to confront and cross-examine a known witness during the trial process is a long-established legal principle. It has only a few, manageable exceptions in relation to absconding accused and unavailable witnesses. As well, there are certain exceptions relating to the hearsay rule. Furthermore, the principle against anonymous testimony relates to matters that are within the inherent domain of the judiciary as a guardian of a judicial system that aims not to convict the innocent.

8.5.3.4 Section 1 of the Charter

If it is accepted that anonymous testimony would violate the principles of fundamental justice, the next question is whether that testimony could in some circumstances nevertheless be justified under section 1 of the *Charter*. No section 7 violation has yet been found by the Supreme Court of Canada to be justified under section 1. Nevertheless, section 1 does apply to section 7 rights, and the courts will consider attempts to justify violations of section 7.[146]

Anonymous testimony in terrorism cases would relate to the objectives of witness protection and making evidence available about a serious crime. Both objectives would be sufficiently important to justify limiting even section 7 rights.

The next question would be whether the use of anonymous testimony would be rationally connected to such objectives. There would be a strong argument for a rational connection to the goal of witness protection because anonymity is the best way to protect witnesses and informers from retaliation. This is recognized in the jurisprudence on informer privilege. As discussed elsewhere in this chapter, no witness protection program provides a complete guarantee of protection. In addition, witness relocation and the need for a new identity divorced from the previous life of the witness impose great hardships. On this basis, using anonymous testimony would likely be found to be rationally connected to witness protection.

---

146 "The *Charter* does not *guarantee* rights absolutely. The state is permitted to limit rights – including the s. 7 guarantee of life, liberty and security – if it can establish that the limits are demonstrably justifiable in a free and democratic society. This said, violations of s. 7 are not easily saved by s. 1": *Charkaoui v. Canada (Citizenship and Immigration)*, 2007 SCC 9, [2007] 1 S.C.R. 350.

Anonymous testimony might also be held to be rationally connected to the objective of making evidence about terrorism crimes available to a court. The Air India investigation is replete with examples of potential witnesses being reluctant to testify for fear that their identities might be disclosed. The only reservation in this respect is the possibility that witnesses would testify even if offered partial anonymity measures such as publication bans on identifying information, the use of screens, remote testimony and entry into a witness protection program.

Whether witnesses could testify without complete anonymity and be protected would be the central consideration in determining whether anonymous testimony constitutes a minimal impairment of the section 7 right. Under this part of the section 1 test, courts would likely require that less drastic alternatives to anonymous testimony either have been tried or would be bound to fail. The UK *Criminal Evidence (Witness Anonymity) Act 2008* addresses this issue by requiring a court to consider "…whether it would be reasonably practicable to protect the witness's identity by any means other than by making a witness anonymity order specifying the measures that are under consideration by the court."[147] A similar requirement would have to be included in any Canadian legislation that hoped to pass the minimal impairment test. Anonymous testimony would not be accepted if less drastic partial anonymity measures were available to protect the witness.

Another less drastic alternative, in light of the 2007 *Charkaoui*[148] decision, would be to allow adversarial challenge to anonymous testimony by a special advocate who would know the identity of the witness. This would respond to some of the difficulties that an accused would face in cross-examining an anonymous witness. However, problems could emerge if the special advocate believed it necessary to communicate with the accused after learning the identity of the witness. The special advocate would not be permitted to reveal identifying information to the accused, but this might mean that the accused could not inform the special advocate of the best grounds to challenge the credibility of the witness. These difficulties would be especially acute where there was a previous but undisclosed relationship between the accused and the anonymous witness.

Courts might also consider witness protection programs to be a less drastic alternative to anonymous testimony. A conclusion that these programs have not been properly funded or administered might suggest that there are still viable alternatives and reforms available short of using anonymous testimony. However, courts would still likely recognize that entry into a witness protection program imposes hardships.

Even if a court accepted that there was no reasonable alternative to anonymous testimony, it would still have to measure the adverse effects on the accused of admitting the testimony against the benefits of allowing its use. Here, courts

147 U.K. *Criminal Evidence (Witness Anonymity) Act 2008*, s. 5(2)(f).
148 *Charkaoui v. Canada (Citizenship and Immigration)*, 2007 SCC 9, [2007] 1 S.C.R. 350.

would probably pay attention to the balance struck by the European Court of Human Rights that anonymous testimony should not be used as the sole or decisive evidence in the case. The Court's approach is based on a weighing of the risk of a miscarriage of justice because of the absence of effective cross-examination, and the unfairness to the accused, against the benefits of testimony from a witness who cannot otherwise provide evidence.[149]

Although it is not possible to predict whether legislation authorizing anonymous testimony would be upheld by the courts, it is clear that courts would not lightly accept such a radical departure from Canadian traditions of a fair trial. They would have to be convinced that there were no less drastic means for protecting witnesses, including various partial anonymity measures such as screens and publication bans, witness protection programs, or permitting special advocates to challenge the anonymous witness. Relevant information possessed by the Crown about the anonymous witness would also have to be disclosed to the accused to assist in the cross-examination, albeit without the information identifying the witness.

Even if no less drastic alternatives were available to make it possible for witnesses to testify, the courts would have to be convinced that, overall, the balance between the harm to the accused and the benefits to society favoured the acceptance of anonymous testimony. At a minimum, Canadian courts would likely follow the European Court ofHuman Rights in not allowing anonymous testimony to be used as the sole or decisive evidence in a prosecution. Canadian courts might well opt for a higher standard that prohibits all anonymous testimony, given the Supreme Court of Canada's treatment of section 7 of the *Charter* and its unwillingness to date to uphold limitations on section 7 rights under section 1.

Even if the courts accepted that anonymous testimony could be justified in some cases, it would be difficult to predict which cases these would be. In every case, less drastic alternatives such as partial anonymity orders would have to be shown to be inadequate. Even if they were inadequate, the benefits of anonymous testimony to the government's objectives of witness protection and prosecuting terrorism cases would have to outweigh the harms of anonymous testimony to the accused.

---

149 These factors are represented in section 5(2) of the U.K. *Criminal Evidence (Witness Anonymity) Act, 2008*, where the judge is instructed to consider:

> (a) the general right of a defendant in criminal proceedings to know the identity of a witness in the proceedings;
> (b) the extent to which the credibility of the witness concerned would be a relevant factor when the weight of his or her evidence comes to be assessed;
> (c) whether evidence given by the witness might be the sole or decisive evidence implicating the defendant;
> (d) whether the witness's evidence could be properly tested (whether on grounds of credibility or otherwise) without his or her identity being disclosed;
> (e) whether there is any reason to believe that the witness—
>
> > (i) has a tendency to be dishonest, or
> > (ii) has any motive to be dishonest in the circumstances of the case,
> > having regard (in particular) to any previous convictions of the witness and to any relationship between the witness and the defendant or any associates of the defendant.

The conditions that would need to be met to justify anonymous testimony would make it very difficult to predict whether anonymous testimony could be used in a particular case. This would make it virtually impossible for CSIS and the police to promise that a person could testify anonymously. Indeed, promises made by the police would have to be carefully framed because a promise of anonymity that was not subsequently accepted by the court under section 1 of the *Charter* might in some cases be interpreted as a promise that would give the potential witness police informer privilege. In such a case, the witness could not be forced to testify without his or her consent. On the other hand, if courts found that the police had not promised anonymity, the witness could be compelled to testify.

Litigating the necessity of anonymous testimony would also lengthen terrorism prosecutions. A decision by a trial judge that anonymous testimony was justified would be open to challenge on appeal. The cumulative effects of non-disclosure are considered on appeal in determining whether an accused's right to make full answer and defence has been violated.[150] The accused could argue that even if the acceptance of anonymous testimony in itself did not make the trial unfair, the anonymous testimony, combined with non-disclosure of other information, could violate the accused's right to make full answer and defence and produce an unfair trial.

8.5.4 Conclusion

Anonymous testimony raises complex issues. Anonymous testimony would be challenged as violating the accused's right to make full answer and defence, including cross-examination, under the *Charter*. The Crown could attempt to justify any violation as a reasonable limit under section 1, but it would have to demonstrate that other measures short of anonymous testimony, such as the use of partial anonymity measures – for example, publication bans, screens or giving testimony from a remote location – would not be adequate. Even then, courts would have to assess the adverse effects of anonymous testimony on the accused's rights, especially in challenging the credibility of the anonymous witness, against the state's interests in securing the anonymous testimony. Of course, Parliament could enact legislation authorizing anonymous testimony notwithstanding the legal rights in the *Charter*. Such legislation would have to be renewed every five years.

Anonymous testimony would not only raise serious *Charter* issues, but also practical issues. Even if Canadian courts followed the European example and allowed anonymous testimony, pre-trial litigation would be necessary to decide whether anonymous testimony was justified. Security intelligence agencies and the police would not know in advance whether anonymous testimony would be allowed. Moreover, the European jurisprudence, as well as the recent British legislation on anonymous testimony, demonstrates a reluctance to allow anonymous testimony to play a decisive role in a criminal prosecution. This reluctance is related to the difficulties that the accused would have in challenging

150 *R. v. Taillefer; R. v. Duguay*, 2003 SCC 70, [2003] 3 S.C.R. 307.

the credibility of an anonymous witness and the dangers of miscarriages of justice. Finally, the nature of clandestine terrorist plots may mean that, regardless of court-ordered anonymity, the accused and their supporters may still be able to determine the identity of an anonymous witness.

Before anonymous testimony can be justified, less drastic measures should be exhausted. Several existing measures protect the identity of informers and witnesses in terrorism cases. Measures discussed elsewhere in this volume, such as the police informer privilege and orders under sections 37 and 38 of the *Canada Evidence Act*, can prevent the disclosure of identifying information about informers who do not testify. Other measures discussed in this chapter can provide partial anonymity and protections against full public disclosure when vulnerable people do testify. The use of pseudonyms may be particularly important in allowing CSIS agents to testify, provided that the Crown makes full disclosure of relevant information about the agent. The robust use of these existing measures can be combined with enhanced and more flexible methods of witness protection.

In light of all the legal and practical difficulties of anonymous testimony, present conditions do not justify a recommendation that the government amend the *Criminal Code* to allow anonymous testimony. However, these conditions may change. The idea that anonymous testimony could be justified in some terrorism prosecutions should not be dismissed out-of-hand. There is ample evidence that witness intimidation frustrated the Air India investigation and prosecution. The government should monitor the use of anonymous testimony under the new British legislation and continue to study the legal and practical implications of witness protection measures including, at the extreme end, the possibility of using anonymous testimony. The government should be prepared to reconsider the present prohibition on anonymous testimony if circumstances warrant.

8.6 Witness Protection Programs

Although there are a variety of measures available to protect the identities of witnesses and sources, there remains a real possibility that some informers and most witnesses will have their identities exposed during testimony. Canada's apparent determination to prosecute terrorism offences also makes it unlikely that the risk of exposing a witness or source would always persuade prosecutors to drop charges.[151] In addition, identity can sometimes be disclosed inadvertently,[152] and the full legal extent of protections from disclosure by means of the police informer privilege and applications for judicial non-disclosure orders under sections 37 and 38 of the *Canada Evidence Act* may not always be clear. As a result, measures are needed to protect those whose identity is

---

151 See Testimony of Raf Souccar, vol. 70, October 31, 2007, p. 8912: "The more serious it [the offence] is, the less discretion would be available."

152 For example, in the Air India investigation, Ms. D's name was released when a warrant application was inadvertently left unsealed by the RCMP commercial crime section. This resulted in her entering the Witness Protection Program much earlier than she had anticipated.

disclosed. This leads to witness protection, a program adopted to manage the consequences of disclosure of the identity of the witness and the resulting risk to the witness and his or her family.

8.6.1 Responsibility for Protecting Witnesses

The protection of witnesses is the responsibility of the police force or agency that intends to rely on that witness. RCMP Assistant Commissioner Raf Souccar testified that, because of the RCMP's leadership role in Integrated National Security Enforcement Teams (INSETs), the RCMP is almost always responsible for protecting witnesses in terrorism investigations. In cases where a source already has a "handler" from another police agency, the source could be transferred to the RCMP and an RCMP handler assigned to the source. As an alternative, the handler from the police agency that first handled the source could be seconded to the RCMP during the investigation.[153]

The practice of seconding a CSIS handler to the RCMP is noteworthy because it may help to avoid the unfortunate treatment received by CSIS sources when transferred to the RCMP during the Air India investigation. For example, Mr. A was transferred from CSIS to the RCMP in March 1987 in an insensitive manner which reduced his possible value as a source of information about Sikh extremism and perhaps as a witness in the Air India prosecution. The handling of Mr. A destroyed the rapport with him achieved by CSIS. Ms. E, who had a good rapport with her CSIS handler, became completely alienated from the authorities after her dealings with the RCMP.

CSIS may have established good relations with sources in the course of previous terrorism investigations. CSIS officers may also have better foreign language skills than their RCMP counterparts and also, perhaps, a greater sensitivity to diverse cultures. Any redesigned system for witness and source protection should permit as much continuity as is feasible in the handling of sources. This is so even if it means that CSIS agents would continue to work with a source who had been transferred to the RCMP and who may eventually testify in a terrorism prosecution. CSIS agents who continue to work with sources must be familiar with, and receptive to, the obligations of disclosure as well as the workings of witness protection programs.

8.6.2 The Federal Witness Protection Program

Because of the central role of the RCMP in witness protection in terrorism investigations, the Commission heard mainly about the protection measures of the RCMP, particularly the federal Witness Protection Program (WPP).

The *Witness Protection Program Act* (WPPA) came into force in 1996, officially establishing the WPP. However, formal witness protection measures in Canada began more than a decade earlier. In 1984, the RCMP established its first major

---

153 Testimony of Raf Souccar, vol. 70, October 31, 2007, pp. 8896-8897.

program, the "Source-Witness Protection Program," because of heightened concern about witnesses in national and international drug smuggling cases. The program had no specific legislative authority. According to author Gregory Lacko, the program was successful in that no protected witnesses ("protectees") were killed while enrolled. However, misunderstandings arose over protection agreements. Some protectees complained, sometimes going as far as sacrificing their anonymity to draw attention to their complaints. Complaints also came before what was then called the RCMP Public Complaints Commission.[154] This led to the enactment of the WPPA in 1996, creating a more formal witness protection regime, the Witness Protection Program (WPP).

Like many of its foreign counterparts[155] and the earlier Source-Witness Protection Program, the WPP was initially established for witness protection needs relating to organized crime.[156] The focus of the WPP continues to be on witnesses who are hardened criminals or who lead a criminal lifestyle.[157]

Under the WPPA, "protection" may include relocation, accommodation and change of identity, as well as counselling and financial support.[158] The purpose of the Act is not simply to facilitate protection for persons assisting the RCMP. The Act also envisages protecting those assisting *any* law enforcement agency or international criminal court or tribunal where an agreement is in place to provide such protection.[159] The Act also contemplates protection for those who act as sources but not as witnesses, though it is generally seen and described as a protection program for witnesses and their close relatives.

The Commissioner of the RCMP or his or her delegate[160] determines whether a witness should be admitted to the WPP and the type of protection to be provided.[161] In practice, the WPP is managed by RCMP Witness Protection Coordinators located across Canada.[162]

The WPPA allows the Commissioner to enter into agreements with other law enforcement agencies to permit a witness to be accepted into the WPP.[163] He may also enter into arrangements with provincial Attorneys General for the same purpose. On the international front (important in the terrorism context),

---

154 Lacko Paper on Protection of Witnesses, p. 3.

155 For example, the American federal witness protection program, also known as the Witness Security Program or WitSec, was established under the *Organized Crime Control Act of 1970*, Pub. L. No. 91-452, 84 Stat. 922, a statute aimed at combatting organized crime.

156 Lacko Paper on Protection of Witnesses, p. 3. The Source-Witness Protection Program became known as the WPP following the enactment of the *WPPA* in 1996.

157 Testimony of Geoffrey Frisby, vol. 70, October 31, 2007, p. 8826. See also Testimony of Mark Lalonde, vol. 68, October 29, 2007, pp. 8615-8616.

158 *Witness Protection Program Act*, s. 2.

159 *Witness Protection Program Act*, s. 3. Section 14 sets out the powers of the RCMP Commissioner and the Minister of Public Safety to enter such agreements.

160 *Witness Protection Program Act*, s. 15.

161 *Witness Protection Program Act*, s. 5.

162 See Testimony of Raf Souccar, vol. 70, October 31, 2007, pp. 8893-8895 for an explanation of the process through which the application of a witness, in this case an RCMP agent, is reviewed by a coordinator and ultimately recommended for admission into the WPP.

163 *Witness Protection Program Act*, s. 14.

the Minister of Public Safety, not the Commissioner, may enter into a reciprocal arrangement with the government of a foreign jurisdiction to enable a witness there to be admitted to Canada's WPP. Similarly, the Minister may make arrangements with international criminal courts or tribunals to admit witnesses from those courts or tribunals to the Program.

As of 2007, there were about 1,000 protectees in the WPP, including 700 managed by the RCMP and 300 from other police forces. About 30 per cent of these protectees were not witnesses, but individuals who had relationships with witnesses.[164]

Other jurisdictions in Canada have created their own witness protection programs – for example, Quebec, Ontario and the City of Montreal. British Columbia established an Integrated Witness Protection Unit in 2003.[165] These programs are independent of one another and, except for the BC program, do not necessarily involve the RCMP.[166] Still, the RCMP can and does on occasion work closely with these programs and it allows officers from these programs to participate in RCMP witness protection training courses.[167]

8.6.3 Hardships Related to Living in the WPP

Souccar testified that entering the WPP is voluntary.[168] This is technically correct. However, the seriousness of threats against those who assist with terrorism investigations and prosecutions may offer little choice but to enter the WPP.

Witnesses before the Commission emphasized the rigours and hazards of life in the WPP. Geoffrey Frisby, a former WPP coordinator, described the program as "very, very difficult" for anyone:

> I don't care who you are; whether you're a hardened criminal with a lengthy criminal record or whether you're an individual who just happened to witness be in the wrong spot at the wrong time. To be able to adjust to the program and to what the program entails, especially when we are looking at having to take a person's identity away from them and give them a new identity. The problems that go with that are increased tremendously with the more protective measures that you provide to an individual.[169]

---

164 House of Commons Canada, Report of the Standing Committee on Public Safety and National Security, *Review of the Witness Protection Program*, March 2008, p. 16, online: Public Works and Government Services Canada <http://dsp-psd.pwgsc.gc.ca/collection_2008/parl/XC76-392-1-1-01E.pdf> (accessed June 2, 2009) [House of Commons Report on the Witness Protection Program].

165 House of Commons Report on the Witness Protection Program, p. 4; Dandurand Paper on Protecting Witnesses, pp. 64-65. Dandurand's description of the integrated BC witness protection unit is an interesting model for consideration, as it appears to integrate municipal police forces and the RCMP under one set of policies.

166 However, the assistance of the WPP is necessary to obtain the federal documents required for a change of identity. See Testimony of Raf Souccar, vol. 70, October 31, 2007, p. 8895.

167 Testimony of Raf Souccar, vol. 70, October 31, 2007, p. 8960.

168 Testimony of Raf Souccar, vol. 71, November 1, 2007, pp. 8974-8975.

169 Testimony of Geoffrey Frisby, vol. 69, October 30, 2007, p. 8794.

RCMP Staff Sergeant Régis Bonneau described undergoing a change of identity and entering the WPP as "…the most stressful things, I imagine, that [protected witnesses and their families] can possibly have to go through in [their lives],"[170] while RCMP Superintendent Michel Aubin characterized the WPP as "a life-altering experience."[171]

The human cost of participation in the WPP was also made clear in *R. Malik and Bagri*, when Justice Josephson described the impact of witness protection on Ms. D:

> She emotionally described how being in the witness protection program had cost her her job, family and contact with friends.[172]

With the help of the RCMP, Commission counsel conducted a survey of WPP protectees to learn more about life under witness protection.[173] The results of the survey and the testimony of witnesses highlighted many hardships that protectees face.

First, protectees are almost inevitably relocated and may have to undergo a change of identity. They often find being uprooted from their home, routine, job and circle of friends particularly difficult. Many protectees report difficulty with the idea of having to "live a lie" for the rest of their lives, and describe how this can inhibit their ability to form lasting relationships in their new location.

Second, protectees generally experience difficulty because of their separation from family members who either were not invited into the WPP or who refuse to enter. Custody arrangements may also prevent a protectee's children from entering the WPP.[174] The WPP can and does organize communication and visits with children of protectees.[175] However, visits are less frequent than most protectees would like and do not come close to approximating the contact with children that parents normally enjoy.[176]

Third, protectees often have difficulty finding employment and becoming self-sufficient in their new location. This often flows from problems in transferring diplomas, work histories and references, as well as their need to receive training in a new field and the heavy demands of their ongoing assistance to the authorities.[177]

---

170 Testimony of Régis Bonneau, vol. 77, November 16, 2007, p. 9781 [translation].
171 Testimony of Michel Aubin, vol. 70, October 31, 2007, p. 8913.
172 *R. Malik and Bagri,* 2005 BCSC 350 at para. 353.
173 See the description of the survey in the statement of Commission counsel Louis Sévéno, vol. 77, November 16, 2007, pp. 9746-9760. See also the accompanying PowerPoint presentation (Exhibit P-298, Tab 1) and report, *Summary, Analysis and Amalgamation of Responses by Protectees of the Federal Witness Protection Program to a Survey Questionnaire* Created by Commission counsel (Exhibit P-298, Tab 2) [Witness Protection Survey].
174 Witness Protection Survey, pp. 16-17, question 43. See also Testimony of Geoffrey Frisby, vol. 70, October 31, 2007, p. 8821.
175 Witness Protection Survey, pp. 10-11, question 26. See also Testimony of Régis Bonneau, vol. 77, November 16, 2007, p. 9775.
176 Testimony of Régis Bonneau, vol. 77, November 16, 2007, p. 9775.
177 Witness Protection Survey, pp. 16-16, questions 39, 42.

Fourth, certain protectees are unable to maintain their earlier lifestyles.[178] WPP administrators will generally liquidate a protectee's assets before proceeding with a change of the protectee's identity. This liquidation can cause a serious loss of capital for the protectee.[179] The WPP strives to follow the "like-to-like" principle and will often provide living allowances to protectees in need. However, the Program is not generally able to match the salary of those witnesses who were well off before.[180]

Finally, most protectees find WPP rules and conditions very difficult to follow, especially restrictions on travelling back to the "danger zone" or contacting friends and relatives in a non-secure manner.[181]

In short, it is almost impossible to overestimate the difficulty and emotional burden of being separated from one's community, and of then having to deny one's entire past and step away from one's roots. Many protectees have left the WPP because of these strict conditions.[182] These conditions, along with the obligation to relocate, are also cited by witnesses who refuse to enter the WPP.[183]

The WPP is also unforgiving, at least on paper. Despite the extraordinary challenges posed by having to remove oneself from one's past, and the understandable desire to maintain some contact with one's former life, the WPPA states that a "deliberate and material contravention of the obligations of the protectee under the protection agreement" can lead to protection being terminated.[184]

The WPP strives to improve the living conditions of protectees and reduce the hardships of life in the WPP. Ways in which the Program can be improved are discussed below. However, several profound hardships that flow from entering and living in the WPP simply cannot be avoided. It is difficult to imagine how the conditions of the WPP could be relaxed, for example, to facilitate a protectee's contact with his or her old community without seriously compromising safety. Even if the Program improves, living under its restrictions will always be a serious challenge for protectees, those who enter the Program with them and those close to the protectee who remain outside the Program. For this reason, the WPP must be viewed as a vital option for protecting witnesses, but almost inevitably one with human costs.

---

178 Witness Protection Survey, p. 14, question 40.
179 Testimony of Raf Souccar, vol. 70, October 31, 2007, p. 8907.
180 Testimony of Régis Bonneau, vol. 77, November 16, 2007, p. 9784.
181 Testimony of Régis Bonneau, vol. 77, November 16, 2007, p. 9787. See also Witness Protection Survey, pp. 18-19, question 52.
182 Testimony of Raf Souccar, vol. 70, October 31, 2007, pp. 8928-8929.
183 Lacko Paper on Protection of Witnesses, p. 15. See also, for example, Exhibit P-273, Tab 10: *Witness Protection Program Act, Annual Report 2005-2006.*
184 *Witness Protection Program Act*, s. 9(1)(b).

8.6.4 Additional Challenges of Living in the WPP in Terrorism Matters

8.6.4.1 Minority Communities

The presence in some ethnic, cultural and/or religious communities of some individuals involved in activities that threaten the security of Canada makes gathering intelligence from within these communities vital. It is essential that the law-abiding majorities in communities be able to provide valuable information to the justice system and that they be protected from intimidation and violence should their assistance become known.

On occasion, the identity of community members who assist security intelligence agencies and the police in terrorism investigations can be kept secret. However, some community members who assist the authorities and testify in terrorism prosecutions may need to enter the WPP. For example, one witness who testified at the Air India trial entered the WPP.[185] It was therefore important for the Commission to assess whether the WPP can meet the needs of individuals from minority communities. Both current and former WPP officials testified about the specific challenges that can arise.

Challenges regarding language skills: Some members of minority communities, especially those who have recently arrived in Canada, may not feel comfortable speaking either of the country's official languages. This makes it more difficult to deal with WPP officials, to understand rights and obligations flowing from a protection agreement, to undergo psychological assessments (a component of the WPP) and to benefit from the services offered through the WPP, such as career counselling and educational programs.

In addition, protectees who were able to live and function normally in their original minority community using their mother tongue may find it impossible to function in a different community where that language is uncommon. This limits the options for relocating protectees.

Souccar told the Commission that to meet the challenge presented by language barriers, the WPP and the RCMP do their best to attract as much diversity as feasible within the WPP to reflect the communities which they serve.[186] Nevertheless, the success of this initiative, established for the entire range of services offered by the RCMP, remains unproven. The initiative constitutes at best a work-in-progress. Souccar also said that the WPP routinely provides protectees with translation services, especially to ensure that they understand the implications of protection agreements.[187] However, these measures do not resolve the difficulties of moving to a community where the protectee's language is not commonly used.

---

185 See *R. v. Malik and Bagri*, 2005 BCSC 350 at paras. 352-353.
186 Testimony of Raf Souccar, vol. 71, November 1, 2007, p. 8971.
187 Testimony of Raf Souccar, vol. 71, November 1, 2007, pp. 8971-8972.

Relocation sites: If the protectee is a member of a visible minority, there may be fewer relocation choices. A protectee would be more easily identified in a small community that lacks others from that minority group. The wearing of traditional or religious garb, as well as distinctive features such as a long beard or tattoos, could increase the risk of being identified.[188] This problem may diminish as Canada, and especially its urban centres, continues to increase in diversity.

Even if a protectee moves to another province, a significant risk of being identified remains. Souccar attributed this to the closeness of some communities across the country:

> It is certainly a challenge depending on the communities, the ethnic communities and their closeness, if you will. The relationship between the same ethnic community in one province perhaps to another. It is a challenge. We work with the individuals who may need protection or relocations to find out what, if any, concern he or she may have in term of relocation and being identified.[189]

However, Bonneau told the Commission that Canada has many large cities in which to relocate members of visible minorities and that this issue was therefore not of particular concern to him.[190]

Limitations on religious freedoms: To reduce the risk to protectees, the WPP generally requires that they not engage in activities that would place them in contact with people who could discover their real identity. This may involve restricting a protectee's place and manner of worship.[191] Because of this, there is a risk that the WPP will be perceived as being insensitive to the cultural and religious customs of minority communities.[192] As well, the pressure to stay away from religious activities could dissuade many who might otherwise help with terrorism investigations and prosecutions. The WPP should be sensitive to these concerns and seek whenever possible to accommodate the religious practices of protectees.

8.6.4.2 Lack of WPP Benefits beyond Protection

Not surprisingly, the evidence before the Commission shows that the major focus of the WPP continues to be on witnesses who are hardened criminals or who lead a criminal lifestyle.[193] These individuals will not see entering the WPP as problem-free, but may recognize it as providing a chance to improve

188 Testimony of Geoffrey Frisby, vol. 70, October 31, 2007, pp. 8832-8833.
189 Testimony of Raf Souccar, vol. 70, October 31, 2007, pp. 8937-8938.
190 Testimony of Régis Bonneau, vol. 77, November 16, 2007, p. 9785.
191 Testimony of Geoffrey Frisby, vol. 70, October 31, 2007, pp. 8832-8833.
192 Testimony of Régis Bonneau, vol. 77, November 16, 2007, pp. 9785-9786.
193 Testimony of Geoffrey Frisby, vol. 70, October 31, 2007, p. 8826. See also Testimony of Mark Lalonde, vol. 68, October 29, 2007, pp. 8615-8616.

their lives and get a fresh start. WPP benefits include drug rehabilitation, career training and counselling.[194] For witnesses who are poor, the WPP ensures a better standard of living.

For those without a criminal past, such as many witnesses and sources in terrorism matters, the benefits mentioned above are less significant (apart from the vital core benefit of protection). Witnesses and sources with no criminal antecedents have fewer reasons than criminals for enduring the hardships of witness protection programs. As a corollary, potential witnesses and sources in terrorism matters have a greater incentive than criminals to withhold useful information from investigators to avoid the need to enter witness protection.

The WPP does not differentiate between the protective measures offered to law-abiding individuals and those offered to career criminals. Souccar testified that, because of its enabling legislation and policies, the WPP's "hands are tied" in the protection that it can offer to "innocent" witnesses, even though WPP officers feel more sympathy for them.[195]

Souccar told the Commission about alternative measures that the police might be able to provide for those who do not enter the WPP, but said that these will often give insufficient protection against a terrorist organization.

All of this points to a need for extra attention within the WPP to make the conditions of the WPP less difficult for witnesses in terrorism cases. In fact, the RCMP has taken steps to soften the harshness of life in the WPP. Measures have included provisions for more frequent visits with family members and the use of systems to ensure safe communications between protectees and those outside the WPP.[196]

8.6.5 Alternative Measures to Protect Witnesses

Because the WPP entails a serious, sometimes intolerable, disruption of the lives of those who require protection, authorities should treat the WPP as the last resort for those at risk, to be used only when less confining protection measures are inadequate or inappropriate.

In fact, the WPPA instructs the RCMP Commissioner to consider "…alternate methods of protecting the witness without admitting the witness to the Program."[197] These alternate methods are not explicitly catalogued in any RCMP policy. However, witnesses told the Commission that a number of measures may be available,[198] according to the level of threat to the witness[199] and the

---

194 Testimony of Geoffrey Frisby, vol. 70, October 31, 2007, p. 8843.
195 Testimony of Raf Souccar, vol. 70, October 31, 2008, pp. 8910-8911.
196 Testimony of Michel Aubin, vol. 70, October 31, 2007, p. 8913. See also Testimony of Raf Souccar, vol. 71, November 1, 2007, pp. 8988-8989.
197 *Witness Protection Program Act*, s. 7(g).
198 Testimony of Raf Souccar, vol. 70, October 31, 2007, p. 8902. See also Testimony of Mark Lalonde, vol. 68, October 29, 2007, pp. 8611-8612.
199 This requires an evaluation of the threat to the witness, a threat assessment, which, in the terrorism context, is likely to be conducted at the INSET level, with the cooperation of all partners.

comfort of the witness with the measures. These measures can be used, for example, where the risk to the witness does not warrant admission to the WPP or where the WPP is not an option, either because the witness refuses to enter or is considered unfit for it.[200]

Security at the home of a witness might be enhanced by an alarm system, surveillance cameras, bars on windows, and by giving the witness and family members emergency emitters ("panic buttons").[201] Witnesses may receive cell phones to facilitate contact with the police, and patrol cars may make frequent rounds in the neighbourhood of the witness.[202] The degree and nature of police presence can vary according to the immediate risk, with an extreme case warranting around-the-clock protection by an emergency response team.[203]

The threat is sometimes limited to a geographical area. Relocation to another neighbourhood may be sufficient to avoid threats from a local gang.[204] In other cases, the need for protection may dissipate with time – after a trial ends, for example. Temporary relocation may resolve the problem here too. However, such measures may not be sufficient in terrorism cases where an extremist organization has a powerful ideological drive, international reach and few scruples about silencing those who work against its interests.

On occasion, a witness who refuses to enter the WPP or is not suitable for the Program is offered a lump sum to pay for private protection services.[205] In exchange, the witness signs an agreement to release the WPP from any protection obligations or further liability. This type of payment arrangement is under some circumstances also offered to witnesses who leave the WPP, but not if payment has already been made for a permanent relocation site.[206]

The lump sum offered to a witness usually equals the WPP's estimate of the cost of protecting the witness (and family) for one year.[207] Souccar testified that, "… [w]e're not going to pay him an amount that is insignificant as compared to what he needs to do to protect himself."[208] An RCMP document showed that between January 1, 2004, and September 13, 2007, 34 witness protection cases were resolved through release and indemnity agreements, with an average payment of $30,000.[209]

---

200 Testimony of Raf Souccar, vol. 70, October 31, 2007, p. 8902.
201 Testimony of Raf Souccar, vol. 70, October 31, 2007, p. 8911.
202 Testimony of Raf Souccar, vol. 70, October 31, 2007, p. 8911. See also Testimony of Mark Lalonde, vol. 68, October 29, 2007, p. 8613.
203 Testimony of Raf Souccar, vol. 70, October 31, 2007, p. 8911.
204 Testimony of Mark Lalonde, vol. 68, October 29, 2007, pp. 8612-8613. See also Testimony of Geoffrey Frisby, vol. 69, October 30, 2007, pp. 8791-8792 and Testimony of Yvon Dandurand, vol. 68, October 29, 2007, pp. 8684-8685.
205 Testimony of Raf Souccar, vol. 70, October 31, 2007, pp. 8931-8932.
206 Testimony of Michel Aubin, vol. 70, October 31, 2007, p. 8929.
207 Testimony of Régis Bonneau, vol. 77, November 16, 2007, pp. 9801-9802.
208 Testimony of Raf Souccar, vol. 70, October 31, 2007, pp. 8931-8932.
209 Exhibit P-273, Tab 12: R&I Payments by RCMP Regional/Divisional SWP Units, January 1, 2004-September 13, 2007.

Witnesses who receive lump-sum payments generally either relocate or implement security measures through private security firms. Using private security firms allows a witness to tailor protection as the witness sees fit. Some witnesses who would balk at the strict conditions of the WPP may be willing to accept private security protection because they have more control over the constraints imposed by the protection.

With private security arrangements, continued protection is not linked to the cooperation of the witness with the police and Crown. However, the cost of private protection can be high, especially where the witness needs around-the-clock protection. A $30,000 lump sum will not go far in such cases. In contrast, witnesses entering the WPP are free of worry about the cost of protection since the RCMP absorbs all costs.

Alternative measures may provide adequate protection in some cases. However, former WPP coordinator Geoffrey Frisby told the Commission that nothing short of admission into the WPP will guarantee the safety of an exposed witness in some situations, and the RCMP will not in such cases offer alternative measures. To do less than what is necessary to make the witness safe, he testified, would be negligent.[210]

Indeed, the single-mindedness of some extremist groups and their willingness to resort to violence to further their objectives means that witnesses and sources whose identities are revealed may often require the extensive protection offered by the WPP. Alternative measures simply may not work.

8.6.6 Organizational Problems in the WPP

8.6.6.1 The Need to Consider the Interests of All Parties in Terrorism Prosecutions

Terrorism investigations and prosecutions can involve many more agencies and departments than other criminal investigations and prosecutions. In gathering intelligence, CSIS will generally play a large role in terrorist investigations and can more easily develop sources in the terrorism milieu than can police agencies. Other agencies may include the RCMP, the National Security Advisor,[211] the proposed Director of Terrorism Prosecutions,[212] federal and provincial Crown prosecutors, Public Safety Canada, Immigration Canada, the Correctional Service of Canada and the Department of Foreign Affairs and International Trade.

Whenever a terrorism prosecution is contemplated, the institutions likely to be affected should be able to express their views about the needs and methods of protecting witnesses and sources. The imposition of expanded disclosure obligations on CSIS as a result of the 2008 *Charkaoui*[213] decision may mean that

---

210 Testimony of Geoffrey Frisby, vol. 70, October 31, 2007, p. 8851.
211 See Chapter II for a discussion of proposals for enhancing the role of the National Security Advisor.
212 See Chapter III for discussion of this proposed position.
213 2008 SCC 38, [2008] 2 S.C.R. 326.

CSIS sources, even if not required to testify, risk being exposed because of a decision by the Crown to prosecute for a terrorism offence. Given the importance that CSIS attaches to keeping the identity of its sources secret, CSIS needs a voice in decisions that might reveal the identity of those sources.

Police and prosecutors may want CSIS intelligence used as evidence by having CSIS sources testify at trial, as happened in the Air India trial. CSIS has a strong interest in ensuring that promises it made to sources, particularly about their anonymity and treatment, are not broken when those sources are transferred to the RCMP. In addition, the value to CSIS of maintaining the anonymity of some sources may exceed the value of those sources for any one particular investigation and prosecution. CSIS may not want to risk ruining ongoing or future intelligence operations about serious threats for the sake of one prosecution. The person holding the enhanced position of National Security Advisor, discussed in Chapter II, will in some cases be able to make decisions about whether preserving the anonymity of CSIS human sources is in the public interest.

If CSIS sources do eventually become witnesses, CSIS will have an interest in ensuring that they receive appropriate witness protection. A failure to provide adequate protection could dissuade others from becoming sources for CSIS and make existing sources reluctant to cooperate further. The CSIS handler may be an important resource in ensuring as smooth a transition as possible from secret human source to witness. There is a need for a person to be in charge and to oversee the transfer of human sources from CSIS to the RCMP as part of the relationship between intelligence and evidence. As discussed later, this person should work closely with both CSIS and the RCMP, but also be independent from the two agencies.

There is also a need to involve prosecutors in matters of witness protection. Prosecutors ultimately make decisions about whether and how to proceed with a prosecution and whether to continue a prosecution in light of a disclosure requirement that may place the life of a witness or source in jeopardy. Prosecutors are responsible for making claims of informer privilege and claims under sections 37 and 38 of the *Canada Evidence Act*. They are also required to justify to the court the use of partial anonymity measures to protect vulnerable witnesses. As discussed in Chapter III, many of these prosecutorial functions in terrorism cases should be performed by the proposed Director of Terrorism Prosecutions.

8.6.6.2 Lack of Firewall between Investigative Units and the WPP

At present, the Commissioner of the RCMP is responsible for the WPP. Because the ultimate decision-making power in the WPP currently resides within the RCMP, which also has an interest in seeing investigations and prosecutions proceed, the lack of an effective "firewall" can create the impression that the interests of the protectee might be sacrificed to serve the ends of an investigation. A perception that the Program is not fair will deter potential witnesses from coming forward.

The RCMP claims to have established a firewall between its investigative and WPP units to ensure the independence of the investigative function from the witness protection function. However, the evidence before the Commission shows that the firewall has not achieved an adequate separation.[214] As a result, investigative units may inappropriately interfere with the protective measures offered to protectees, to their detriment.

The House of Commons Standing Committee on Public Safety and National Security recommended that the RCMP not make decisions about witness admission and protection agreements, but that it should be responsible for threat assessments, determining the necessary level of security and implementing protective measures.[215]

8.6.6.3 Inadequate Conflict Resolution Mechanisms

The very nature of witness protection implies a significant power imbalance between the protectees and those protecting them. This imbalance permeates the current conflict resolution and complaints process.[216] Protectees require RCMP assistance to remain safe, so they are naturally reluctant to raise complaints about the way the RCMP runs the WPP. Dandurand testified that one of the main challenges of conflict resolution in the WPP is that protectees find themselves in conflict with the organization that affords them the protection they need.[217] Since all current methods of dispute resolution are initiated by the protectees, Dandurand maintained, protectees will be reticent about asserting their rights. Asserting rights through a complaint amounts to "biting the hand that feeds them."[218] [translation]

The conflict resolution process for protectees begins at the level of the WPP handler or coordinator, where most disagreements can be resolved.[219] However, if a protectee is not satisfied by a decision taken at this level, the complaint

---

214 Geoffrey Frisby testified that, in his experience, the policy of a strict firewall between protective and investigative units is "not real at all": Testimony of Geoffrey Frisby, vol. 70, October 31, 2007, p. 8827. Frisby spoke of instances of contact between investigators and their protected witnesses in which the investigators attempted to sway a WPP unit's decision regarding a given witness and his/her treatment: Testimony of Geoffrey Frisby, vol. 70, October 31, 2007, pp. 8825-8826. Régis Bonneau also described communications between investigators and witness protection to resolve conflicts as "an avenue that's used regularly" [translation]: Testimony of Régis Bonneau, vol. 77, November 16, 2007, p. 9792. Furthermore, the funding for the protection measures extended to a given protectee comes from the investigative budget. This further decreases the independence of the WPP from the rest of the RCMP: see, for example, Testimony of Régis Bonneau, vol. 77, November 16, 2007, pp. 9800-9801. Finally, the Commission heard that what little independence may exist at the level of the coordinators is nearly erased at the upper levels of the RCMP, since the officers who are ultimately responsible for the WPP, the Commissioner and the Assistant Commissioner, Federal and International Operations, also oversee the operations of investigative units: Testimony of Anne-Marie Boisvert, vol. 69, October 30, 2007, p. 8756.

215 House of Commons Report on the Witness Protection Program, p. 26.

216 Testimony of Paul Kennedy, vol. 70, October 31, 2007, p. 8875.

217 Testimony of Yvon Dandurand, vol. 69, October 30, 2007, p. 8703.

218 Testimony of Yvon Dandurand, vol. 69, October 30, 2007, p. 8704.

219 Testimony of Régis Bonneau, vol. 77, November 16, 2007, pp. 9790-9791. According to Bonneau, roughly 50 per cent of all complaints are resolved at this level.

may be addressed to more senior officers of the WPP/RCMP, and make its way eventually to the Commissioner or his or her delegate.[220] Bonneau estimated that roughly 75 per cent of all protectee complaints can be resolved within the RCMP.[221]

For those issues that cannot be resolved within the RCMP to a protectee's satisfaction, the protectee may complain to the Commission for Public Complaints Against the RCMP (CPC). However, this option is often of little use to the protectee, since the CPC does not generally receive full access to the documents it might require to render a decision. Furthermore, its decisions are not binding on the RCMP Commissioner, who may substitute findings of fact or simply ignore the decision. For these reasons, the CPC does not appear to be the ideal venue for complaints from protectees in terrorism matters.

The only option today for a protectee to obtain a decision that binds the RCMP is to take time-consuming legal action. This usually involves either filing a civil action in provincial courts or presenting a *certiorari* or *mandamus* motion in the Federal Court. Adding to this problem is the lack of readily available legal advice on the merits of complaints against the RCMP.

Any new witness protection program should aim to render unnecessary any reliance on either the CPC or litigation. A new program should be more witness-centred and take the interests of witnesses into account in protection matters. It should also include dispute resolution mechanisms that respect the absolute need for confidentiality in witness protection matters.

There should be continuity with respect to dispute resolution so that a single grievance, that might not seem serious if viewed in isolation, can be seen in the broader context of the protectee's entry and history in the Witness Protection Program. As has been suggested, an independent person could play an ombudsperson's role in resolving disputes about protection.[222] In addition, private and binding arbitration by a retired judge or other respected individual, preferably legally trained, could also play a role. A binding arbitration clause could be included in protection agreements that would prevent protectees from litigating their disputes in the courts, at least at first instance, in exchange for an efficient, credible and confidential system of dispute resolution. Such an approach is especially necessary in the terrorism context, where sensitive national security matters might complicate the resolution of protectee concerns.

8.6.6.4 The Need to Restructure the WPP in Terrorism Matters

The current WPP model is ill-suited for terrorism matters for the three main reasons described earlier:

---

220 Testimony of Régis Bonneau, vol. 77, November 16, 2007, pp. 9790-9791. Currently, the Commissioner's delegate, according to s. 15 of the *Witness Protection Program Act*, is the RCMP's Assistant Commissioner, Federal and International Operations.

221 Testimony of Régis Bonneau, vol. 77, November 16, 2007, p. 9791. According to Bonneau, roughly 50 per cent of all complaints are resolved at the level of the handler and coordinator, while another 25 per cent are resolved by officers in the upper echelons of the RCMP.

222 Testimony of Mark Lalonde, vol. 68, October 29, 2007, pp. 8651-8652.

- The WPP is not equipped to provide continuity in the handling of CSIS sources who may become witnesses;

- The approach of the WPP is too rigid to respond to the varying needs of witnesses in terrorism cases and is based on an implicit assumption that most protectees have a criminal background; and

- The management functions of the WPP lack independence from the investigative teams within the RCMP.

These reasons provide a strong case for the adoption of a terrorism-specific approach when dealing with the witnesses and sources who may help in terrorism investigations and prosecutions. They also point to a need to facilitate the interagency cooperation that is essential for effectively dealing with terrorism.

8.6.7 A New Body to Manage Witness Protection: A National Security Witness Protection Coordinator

Recent reviews of witness protection issues have favoured establishing a separate body to administer and manage the WPP. For example, the House of Commons Standing Committee on Public Safety and National Security recommended this approach its March 2008 report:

> [E]ntrust the administration of the Witness Protection Program to an independent Office within the Department of Justice. A multidisciplinary team from the Office, which could consist of police officers, Crown attorneys and psychologists and/or criminologists with appropriate security clearance, should be responsible for making decisions about witness admission and for monitoring of protection agreements. Police forces should be responsible for threat assessments, determining the level of security and implementing the protective measures.[223]

The Standing Committee reasoned that a multidisciplinary team would be in a much better position to "…strike a balance between the public interest (vis-à-vis the risk posed by a witness's participation in the Program) and the interests of the prosecution (from the police standpoint)."[224] The Committee referred to the testimony before it of Nick Fyfe, Director of the Scottish Institute for Policing and Research and Professor of Human Geography. Fife testified that "…having that kind of group taking those decisions, one that is slightly removed from the police, may offer a more independent and perhaps more dispassionate view of whom it is appropriate to protect and who would be included and who should be excluded from these programs."[225]

---

223 House of Commons Report on the Witness Protection Program, p. 26.
224 House of Commons Report on the Witness Protection Program, pp. 25-26.
225 House of Commons Report on the Witness Protection Program, p. 26.

Dandurand, former police officer Mark Lalonde and Boisvert also stated their support for reform similar to that proposed by the Standing Committee.[226] Dandurand testified that an independent organization would enhance the image and credibility of the WPP. Individuals who were considering cooperating in an investigation or prosecution would immediately know that they were dealing with an organization that had a mandate to protect them, rather than simply to conduct investigations. "[I]n terms of perceptions," he testified, "it is crucial."[227] [translation]

Separate administration of witness protection matters may also enhance the credibility of witnesses. The fact that a witness receives money for assistance or a living allowance for protection may undermine the credibility of the witness at trial. The defence may argue that the testimony of the witness is being "bought" by the police or the Crown. However, there will be less merit in such claims if a separate body decides the awards and living allowances. Such a separate body, headed by a person who inspires public confidence, may also be able to explain the need for protection measures including, when necessary, lump sum payments. The person heading this body should not hesitate to speak out about the difficult situations experienced by some witnesses, as well as of the vital public service that witnesses provide.

Some parties before the Commission rejected the notion of a separate body to administer witness protection. For example, Souccar argued that only the police have the experience and expertise to handle and protect human sources, and also to admit them to and terminate them from the WPP.[228] He was satisfied that, although some improvements were warranted, the WPP was working well and that "it's not broken." In its Final Submission, the Air India Victims Families Association (AIVFA) recognized the need for independence of the investigative and protective units, but argued that an independent agency would lack expertise and that it did not make sense to create one.[229]

The core logic in proposals for a new agency is to insulate decisions about protection of witnesses from decisions about investigations and prosecutions. Decisions about witness protection have direct implications which go beyond policing, affecting in particular the rights and interests of the witnesses and, more broadly, the administration of justice. Boisvert argued that it would be inappropriate to leave decisions about using the services of a witness and offering witness protection in the hands of the police exclusively:

> When you want to establish procedures and use the services of a collaborator for whom the human cost will be significant, a decision must be made as to how justice can best be

---

226 Testimony of Yvon Dandurand, vol. 69, October 30, 2007, pp. 8707-8708; see also Testimony of Mark Lalonde, vol. 68, October 29, 2007, pp. 8652-8653 and Testimony of Anne-Marie Boisvert, vol. 69, October 30, 2007, pp. 8745, 8765.

227 Testimony of Yvon Dandurand, vol. 69, October 30, 2007, p. 8735.

228 Testimony of Raf Souccar, vol. 71, November 1, 2007, pp. 8968-8969.

229 AIVFA Final Written Submission, pp. 171-172.

> served. An analysis must be conducted … a cost-benefit analysis naturally, but also an analysis of the human cost and the decision's impact on the administration of justice. In my opinion, this decision should not be left to just the police. The police are certainly major players. They have significant expertise, but it seems to me that it isn't for the police to determine, on their own, whether to use a witness who will then have to be protected, and whether, ultimately, the case will be prosecuted.[230] [translation]

Many jurisdictions, including Belgium,[231] Italy[232] and Quebec, use a multidisciplinary approach to witness protection, an approach also supported by the recent House of Commons Standing Committee on Public Safety and National Security.[233]

In Quebec, witness protection decisions were recently removed from the Sûreté du Québec, although it continues to provide physical protection. Decisions about other aspects of protection are now made by a committee with representatives from four agencies: the Department of Justice (Québec), the police force that recruited the witness, the Ministère de la sécurité publique and the Direction générale des services correctionnels.[234] No prosecution may use the testimony of a "collaborator" witness until a protection agreement is negotiated with the committee.

In terrorism matters, the bodies likely to have the interest and expertise to be involved in decisions regarding witness protection include the RCMP, CSIS, the National Security Advisor (Privy Council Office), the federal Department of Justice as represented by the proposed Director of Terrorism Prosecutors, Public Safety Canada, Immigration Canada, the Correctional Service of Canada and, especially when international agreements are involved, the Department of Foreign Affairs and International Trade.

There is a danger that putting representatives of each of these agencies on a committee that has decision-making power might result in bureaucracy and delay. This would be dangerous, given that decisions in terrorism matters

---

230 Testimony of Anne-Marie Boisvert, vol. 69, October 30, 2007, p. 8765.

231 In Belgium, the Witness Protection Commission, an independent agency comprising representatives from the Attorney General, the King's Counsel, the General Directorate for Operational Support, the Ministry of Justice and the Ministry of the Interior, decides any matters relating to the extension, modification or removal of protective measures for witnesses, as well as financial awards/aid. See Anne-Marie Boisvert, "La protection des collaborateurs de la justice: éléments de mise à jour de la politique québécoise" (June 2005), p. 20, online: Sécurité publique Québec <http://www.msp.gouv.qc.ca/police/publicat/boisvert/rapport_boisvert_2005.pdf> (accessed June 2, 2009) [Boisvert Report on the Protection of Justice Collaborators].

232 In Italy, the Central Witness Protection Commission makes the decisions to admit or refuse witnesses, based on recommendations from government prosecutors. Another agency, the Central Witness Protection Service, is responsible for the practical aspects of the program. This last agency is part of the Criminal Police Central Directorate, which answers to the Department of Public Security: Boisvert Report on the Protection of Justice Collaborators, p. 20.

233 House of Commons Report on the Witness Protection Program, pp. 25-26.

234 See Boisvert Report on the Protection of Justice Collaborators, p. 14.

may have to be made quickly. For example, an intelligence investigation may discover evidence of criminality and quickly have to be converted into a criminal investigation. Arrangements for the protection of CSIS sources may have to be made quickly in such cases. Even where the Crown will assert police informer and other privileges, the National Security Witness Protection Coordinator will need to have contingency plans that can be implemented quickly should identifying information about a human source be disclosed.

To ensure quick and decisive action, the Commission calls for the creation of a position of "National Security Witness Protection Coordinator" to deal with witness protection issues in terrorism matters. Wherever possible, this person should consult closely with the various agencies listed above. In almost all cases, the Coordinator will have to work very closely with CSIS, the RCMP and prosecutors. At the same time, the Coordinator should be independent of all these agencies and have ultimate power to make decisions in witness protection matters.

The National Security Witness Protection Coordinator would generally become involved after a decision has been made to commence a terrorism prosecution that would require witness and source protection. The National Security Advisor[235] may have already carefully examined the case and may have even consulted the National Security Witness Protection Coordinator to obtain independent advice about witness protection options. In appropriate cases, the National Security Advisor may have made a decision, such as that made in the post-bombing investigation in the Air India case, that CSIS sources should be made available to the RCMP.

The National Security Witness Protection Coordinator's mandate would include:

- assessing the risks to potential protectees resulting from disclosure and prosecutions, as well as making decisions about accepting an individual into the Witness Protection Program and the level of protection required;
- working with relevant federal, provincial, private sector and international partners in providing the form of protection that best satisfies the particular needs and circumstances of protectees;
- ensuring consistency in the handling of sources and resolving disputes between agencies that may arise when negotiating or implementing protection agreements (this function would be performed in consultation with the National Security Advisor);
- providing confidential support, including psychological and legal advice, for protectees as they decide whether to sign protection agreements;
- negotiating protection agreements, including the award of payments;

---

235 As explained in Chapter II.

- providing strategic direction and policy advice on protection matters, including the adequacy of programs involving international cooperation or minors;
- providing for independent and confidential arbitration of disputes that may arise between the protectee and the program;
- making decisions about ending a person's participation in the program;
- acting as a resource for CSIS, the RCMP, the National Security Advisor and other relevant agencies about the appropriate treatment of sources in terrorism investigations and management of their expectations;
- acting as an advocate for witnesses and sources on policy matters that may affect them and defending the need for witness protection agreements in individual cases.

The National Security Witness Protection Coordinator would not be responsible for providing physical protection. That function would remain with the RCMP or other public or private bodies that provide protection services and that agree to submit to confidential arbitration of disputes by the Coordinator.

The Coordinator would not recruit sources or make decisions about the coordination of intelligence or the appropriateness of criminal prosecutions. Such matters would fall to the National Security Advisor and to the appropriate prosecuting authorities. The Coordinator could, however, provide advice to the National Security Advisor and to prosecutors about options for witness protection.

The position of the National Security Witness Protection Coordinator would be recognized in amendments to the *Witness Protection Program Act*. These amendments would also mean that the RCMP Commissioner would no longer administer the Witness Protection Program in national security matters.

The National Security Witness Protection Coordinator should be a respected, independent individual, such as a retired judge, who would be chosen for his or her knowledge and experience in criminal law, national security issues and witness protection. He or she could consult widely, but ultimately would have the power to make final and binding decisions about witness protection in terrorism cases.

The Coordinator should provide an impartial public interest perspective in disputes between intelligence and police agencies. Perhaps as important, the Coordinator could serve as a voice for the witnesses and sources whose lives may be so profoundly affected by matters of witness protection. Finally, the Coordinator could press the government for appropriate resources and cooperation in witness protection matters. The Coordinator would have ready access to the National Security Advisor. In cases where the National Security Advisor had made decisions involving the transfer of sensitive sources from CSIS to the RCMP, the Coordinator would work closely with CSIS and the RCMP to

ensure that the transition would be as smooth as possible. This is the minimum required if intelligence provided by secret CSIS sources is to be converted into testimony in a terrorism prosecution.

The Coordinator's independence would allow him or her to defend the terms of witness protection agreements. Because the police would have no control over administration of witness protection, there would be no appearance that the police were "buying" testimony through an offer of witness protection.

The Coordinator should stress flexibility and the need for quick and decisive action in matters of witness protection. The Coordinator should not take a "one-size-fits-all" approach to protection. He or she should look at each case and try to devise workable and sustainable protection agreements that minimize the considerable hardships relating to life under witness protection.

Life under the WPP will never be easy, and the National Security Witness Protection Coordinator should consider alternative protection measures, including international transfers, lump sum payments and arrangements with the private sector. Such measures may in some cases be just as effective in providing safety and peace of mind for witnesses as their entry into a life-changing witness protection program. The Coordinator should consider the least restrictive protective options that provide sufficient protection. He or she should be a creative, hands-on presence in matters of witness protection.

The RCMP and CSIS will, of course, remain free to develop their own sources and agents. However, the National Security Witness Protection Coordinator, perhaps in consultation with the proposed Director of Terrorism Prosecutions, could provide guidance to the agencies that would discourage handlers from acting improperly, such as by using deceit, showing insensitivity about problems that witnesses and sources encounter, and making inappropriate or unrealistic promises of anonymity. The Coordinator could also conduct "lessons learned" analyses of past cases to enable the agencies to make better source handling decisions in the future.

Although some aspects of witness protection agreements for those who testify may be subject to disclosure under the broad disclosure rights set out in *Stinchcombe*[236] or as records held by third parties under *O'Connor*,[237] other aspects may be covered by informer privileges or by specified public interest or national security privileges under sections 37 and 38 of the *Canada Evidence Act*. In addition, section 11 of the *Witness Protection Program Act* prohibits the direct or indirect disclosure of the location or change of identity of a person who is in or has been in the WPP, subject to limited exceptions including when the innocence of the accused is at stake.

---

236 [1991] 3 S.C.R. 326. See Chapter V for a discussion of the breadth of such disclosure obligations. For an application of *Stinchcombe* with respect to witness protection matters, see *R. v. McKay*, 2002 ABQB 335.

237 [1995] 4 S.C.R. 411. See Chapter V for a discussion of these procedures for obtaining records from a third party not subject to *Stinchcombe*. For an application of *O'Connor* with respect to witness protection matters, see *R. v. James; R. v. Smith*, 2006 NSCA 57, 209 C.C.C. (3d) 135.

For purposes of the informer privilege, the National Security Witness Protection Coordinator should be considered a part of law enforcement, and it should be clear that the passing of information to the Coordinator would not in itself defeat claims of informer privilege.[238]

The assignment of powers to the National Security Witness Protection Coordinator to make witness protection decisions avoids the danger of creating one more layer of bureaucracy that might be required should an interdisciplinary and multi-agency committee have the power to make decisions. The Coordinator could and should consult with multiple agencies.

There should be firm time limits for decisions about witness protection. The requirements for witness protection must be widely known and generous. The most efficient organizations to spread the knowledge would be agencies such as the RCMP and CSIS.

8.6.7.1 Judicial Review of the National Security Witness Protection Coordinator's Decisions

In the absence of a privative clause, the National Security Witness Protection Coordinator's work could be subject to judicial review pursuant to the *Federal Courts Act*.[239] In the Commission's view, the decision by the Coordinator to admit or refuse a person entry into a witness protection program should not be subject to judicial review. Still, there may be a role for judicial review of disputes between protectees and those who administer the program, but only after they have exhausted an internal and confidential mediation and arbitration processes.

8.6.7.2 The Decision to Admit or Refuse Entry to Witness Protection

Admission to witness protection must advance the particular investigation and also be in the public interest. To assess the public interest, a broad set of factors must be considered.

The factors will vary from case to case. An RCMP witness seeking protection may have been a source for CSIS in the past, which may limit the viability of that person as a witness. There may also be international implications to providing protection where a witness is being targeted by a foreign service or is wanted by a foreign law enforcement agency, or where the witness may ultimately be moved out of Canada to afford protection. It may also be necessary to assess the proposed evidence of the witness, both to determine its value to the prosecution and to assess whether it could reveal sensitive information. These factors involve considering sensitive issues that render judicial review inappropriate.

---

238 See also Chapter IV, where it is suggested that the passing of information from CSIS to law enforcement officials under s.19 of the *CSIS Act* should not in itself defeat any subsequent claims of informer privilege.

239 R.S.C. 1985, c. F-7.

It ought to be the purview of the Coordinator to decide on protection by taking into account the exigencies of the particular investigation and the impact of such a decision across a variety of interests. This decision must be free from judicial review and interference. The judiciary is not part of the investigative machinery of the state, save to protect individuals from state excess.[240] Absent a potential constitutional infringement, the judiciary should not sit in review of decisions about how to conduct an investigation.

No person has a right to be admitted to a witness protection program. The decision to admit does not engage any constitutional issues. It rests solely within the discretion of the state.

Some applicants will be disappointed if they are refused admission. That should not give rise to a legal right to challenge the refusal. The reasons for refusing admission will often involve strategic issues of national security that cannot be disclosed to the person – nor should they be disclosed. This is not akin to seeking a government benefit where there is some entitlement to that benefit. This program is an investigative device to support national security investigations, not an entitlement. Viewed in that light, it is obvious that judicial review is inappropriate.

For this reason, there should be a privative clause prohibiting both judicial review of and appeals from the decision of the National Security Witness Protection Coordinator to admit or refuse to admit an individual into the witness protection program.

8.6.7.3 Dispute Resolution

When being admitted to the WPP, the protectee must come to an agreement about the terms of protection. These terms will identify the respective legal obligations, entitlements and duties of the protectee and the program including, in most cases, the RCMP.

During the period of protection, disputes may arise between the RCMP and the protectee. There must be a dispute resolution mechanism to deal with the myriad of issues that may arise. It would make sense for the National Security Witness Protection Coordinator or a person delegated by the Coordinator, rather than the courts, to address these disputes. The Coordinator might wish to delegate binding decisions to a third party to enable the Coordinator to serve as an ombudsperson or a mediator.

It is important that there be continuity with respect to dispute resolution. The same person should resolve all disputes between a given protectee and the RCMP. Continuity ensures that disputes are viewed not only in light of the current situation, but also in light of the history of the file. This ensures the long-term

---

240 This is the constitutional justification for prior judicial authorization for invasions of privacy. Certainly, the judiciary determines if the state will be permitted the investigative tool that invades privacy (for example, a search warrant). However, that is a necessary byproduct of protecting the individual's right to privacy.

viability of protection in a given case. For this reason, all protectees should have to accept that all disputes be dealt with in the first instance by the Coordinator or the Coordinator's delegate.

The Coordinator should have the authority to determine the process by which disputes are resolved. The process should be flexible, not formal and "court-like." Given the interests at stake, a private arbitration of the dispute is the most appropriate way to ensure that the various interests are represented and issues resolved. Privacy will often be necessary to ensure the safety of the protectee and protect the state's interest in safeguarding sensitive information.

There must be sufficient substantive protections for the protectee. At a minimum, the protectee should be represented by counsel, if desired, and be provided an opportunity to be heard. This would include the right to put supporting information before the Coordinator or the person designated by the Coordinator to address disputes. If the protectee could not afford counsel, the federal government should cover the cost in accordance with Treasury Board guidelines.

Given that the adjudication of rights and obligations is involved, it is appropriate for the dispute resolution decisions of the Coordinator or his or her delegate to be reviewable by the Federal Court pursuant to section 18 of the *Federal Courts Act*. Although the Court would determine the nature of the review, considerable deference ought to be afforded to the arbitration process developed by the Coordinator. In dealing with protection matters, the Coordinator would have expertise akin to that of many specialized tribunals that operate within federal jurisdiction. It is important that the Coordinator be afforded the flexibility to devise the process and that rules of evidence not frustrate the process. With these principles in mind, the aims of the witness protection program and the reasonable concerns of the protectee can be harmonized. However, judicial review is appropriate as an ultimate safeguard to ensure that substantive protections are afforded to the parties.

Recommendation 24:

A new position, the National Security Witness Protection Coordinator, should be created. The Coordinator would decide witness protection issues in terrorism investigations and prosecutions and administer witness protection in national security matters. The creation of such a position would require amendments to the *Witness Protection Program Act*.

The National Security Witness Protection Coordinator should be independent of the police and prosecution. He or she should be a person who inspires public confidence and who has experience with criminal justice, national security and witness protection matters.

Where appropriate and feasible, the Coordinator should consult any of the the following on matters affecting witness and source protection: the RCMP, CSIS, the National Security Advisor, the proposed Director of Terrorism Prosecutors,

Public Safety Canada, Immigration Canada, the Department of Foreign Affairs and International Trade and the Correctional Service of Canada. The Coordinator would generally work closely with CSIS and the RCMP to ensure a satisfactory transfer of sources between the two agencies.

The National Security Witness Protection Coordinator's mandate would include:

- assessing the risks to potential protectees resulting from disclosure and prosecutions, as well as making decisions about accepting an individual into the witness protection program and the level of protection required;
- working with relevant federal, provincial, private sector and international partners in providing the form of protection that best satisfies the particular needs and circumstances of protectees;
- ensuring consistency in the handling of sources and resolving disputes between agencies that may arise when negotiating or implementing protection agreements (this function would be performed in consultation with the National Security Advisor);
- providing confidential support, including psychological and legal advice, for protectees as they decide whether to sign protection agreements;
- negotiating protection agreements, including the award of payments;
- providing strategic direction and policy advice on protection matters, including the adequacy of programs involving international cooperation or minors;
- providing for independent and confidential arbitration of disputes that may arise between the protectee and the witness protection program;
- making decisions about ending a person's participation in the program;
- acting as a resource for CSIS, the RCMP, the National Security Advisor and other agencies about the appropriate treatment of sources in terrorism investigations and management of their expectations;
- acting as an advocate for witnesses and sources on policy matters that may affect them and defending the need for witness protection agreements in individual cases.

The National Security Witness Protection Coordinator would not be responsible for providing the actual physical protection. That function would remain with the RCMP or other public or private bodies that provide protection services and that agree to submit to confidential arbitration of disputes by the Coordinator.

8.6.8 Other Issues Relating to Witness Protection in Terrorism Cases

8.6.8.1 International Agreements

Relocating some witnesses within Canada may not protect them sufficiently. The WPPA allows the Minister of Public Safety to enter into a reciprocal arrangement with the government of a foreign jurisdiction which would enable a witness to be relocated to that jurisdiction.[241] Two such agreements were signed as of April 2007, and a further two with international tribunals in June of that year.[242] However, Souccar testified that Canada's size allowed it to "…relocate and ensure the safety of an individual…in Canada fairly well." A more typical situation would be for other countries to seek to transfer their protectees to Canada.[243] As of June 2007, 27 foreign protectees had been admitted to Canada's WPP.

Once a Canadian witness is enrolled in a foreign witness protection program, the Canadian WPP cannot address the safety concerns of that witness as capably as if the witness were in Canada. Accordingly, WPP officials must have confidence in the foreign program before relocating a witness.[244] Dandurand testified that it is not easy to evaluate the trustworthiness of foreign police forces, programs and public servants, but that RCMP liaison officers abroad should be able to help.[245]

It is likely that international relocation will be considered only in very exceptional circumstances. The witness may be needed during trial preparation and testimony, which can last many years, so international relocation during that period would not be practical. For a Canadian protectee, adapting to a life in a foreign country may be even more difficult than adapting to a life elsewhere in Canada. In addition, there are administrative challenges to transferring a protectee. Nonetheless, international relocation remains a possibility and has been used in several cases.

If the Minister of Public Safety makes arrangements with additional foreign jurisdictions, Canadian protectees will benefit from a wider range of choices for relocation. This is likely to be particularly beneficial for protectees from certain ethnic, cultural or religious communities because the added choice may help them to find an environment in which they are comfortable. For this reason, the Commission encourages the Minister of Public Safety to explore further international arrangements under section 14 of the WPPA.

---

241 *Witness Protection Program Act*, s. 14(2).

242 Exhibit P-274, Tab 5: Letter, June 27, 2007, signed on behalf of Beverley A. Busson, RCMP to Gary Breitkreuz, President, House of Commons Standing Committee on Public Safety and National Security, p. 1. Section 14(3) of the *Witness Protection Program Act* allows the Minister of Public Safety to enter into an arrangement with an international criminal court or tribunal.

243 Testimony of Raf Souccar, vol. 70, October 31, 2007, p. 8938; Testimony of Raf Souccar, vol. 71, November 1, 2007, pp. 8977-8978.

244 Testimony of Raf Souccar, vol. 71, November 1, 2007, pp. 8977-8978.

245 Testimony of Yvon Dandurand, vol. 69, October 30, 2007, pp. 8697-8698.

8.6.8.2 Independent Legal Advice for Protectees

As noted earlier, witnesses negotiating entry into the WPP do so from a position of weakness, since they are highly dependent on the protection that the WPP can offer.[246] They are often frightened by the threats they face and may not fully understand how entering the program will affect their lives. They may feel pressure to accept a protection agreement as it is presented to them, and they may also lack the understanding to ask important questions about their rights and obligations and the obligations of others.

Souccar testified that the protective measures provided by the WPP cannot be "negotiated down" to less than those required to ensure the safety of the protectee. However, several other important aspects of the protection agreement can be negotiated.[247] Examples include the living conditions of the protectee,[248] the relocation site,[249] visitation rights and the frequency of family visits[250] and the number of family members who may be admitted to the WPP.[251]

Several witnesses before the Commission called for protectees to have access to independent legal advice.[252] In its March 2008 report on the WPP, the House of Commons Standing Committee on Public Safety and National Security reached a similar conclusion.[253]

Some officials told the Commission that independent legal advice was being made available to prospective protectees, but this claim conflicted with the findings of the survey[254] of protectees conducted by Commission counsel (with the assistance of the RCMP) and with the recent report of the Standing Committee. That report stated that, at present, potential protectees negotiating with the RCMP for protection are not offered the services of a lawyer.[255] As well, Commission counsel examined several versions of the Sample Protection Agreement.[256] Only one version mentioned the availability of independent legal advice for the protectee. None of the agreements contained a clause for the protectee to indicate that he or she had either obtained or declined such advice.

The WPP should ensure that individuals are informed in writing, where practical, about the availability and importance of independent legal advice, and explain

---

246 Testimony of Yvon Dandurand, vol. 69, October 30, 2007, p. 8701.
247 Testimony of Raf Souccar, vol. 70, October 31, 2007, pp. 8924-8925.
248 Testimony of Régis Bonneau, vol. 77, November 16, 2007, p. 9810.
249 Testimony of Raf Souccar, vol. 71, November 1, 2007, p. 8950.
250 Testimony of Régis Bonneau, vol. 77, November 16, 2007, p. 9775.
251 Testimony of Raf Souccar, vol. 70, October 31, 2007, p. 8908.
252 Testimony of Anne-Marie Boisvert, vol. 69, October 30, 2007, p. 8761; see also Testimony of Yvon Dandurand, vol. 69, October 30, 2007, pp. 8700-8701.
253 House of Commons Report on the Witness Protection Program, p. 28.
254 The general findings of this survey are discussed above. Some 62 per cent of respondents stated that they had not been offered independent legal advice during the negotiation of their protection agreement.
255 House of Commons Report on the Witness Protection Program, p. 27.
256 See Exhibits P-273, Tab 1 and P-274, Tabs 3, 7, 8.

that the WPP will pay the reasonable costs of the advice.[257] In addition, protection agreements should be revised to include a clause for the prospective protectee to sign confirming that he or she has been advised of the availability of free independent legal advice and that the advice was either obtained or declined.

It may be necessary as well to require that counsel be security-cleared, since counsel might need access to information covered by national security privilege in order to advise the protectee knowledgeably.

Independent legal advice could equally be warranted for other agreements involving witnesses at risk, such as a release and indemnity agreement. It would also be useful in dealing with a notice of termination from the WPP, particularly where termination might jeopardize the protectee's safety.

8.6.8.3 Psychological Evaluations

Several RCMP officials[258] testified about the psychological challenges of life in the WPP. As well, Dandurand told the Commission that the limited research on this topic revealed that protectees often "…find … themselves quite depressed and despondent and having a very difficult time adapting." Dandurand concluded that this caused many protectees to withdraw from the WPP.[259]

Psychological assessments can help to evaluate a protectee's capacity to adapt to the rigours of the WPP. They can detect signs of depression, the risk of suicide and substance abuse problems. The WPP provides psychological help to protectees after they join the WPP if they request or accept assistance. However, psychological assessments before entry to the WPP are not conducted as frequently as required. Section 7 of the WPPA obliges the RCMP Commissioner to consider a range of factors to determine whether prospective protectees are admitted the WPP. One factor is "…the likelihood of the witness being able to adjust to the Program, having regard to the witness's maturity, judgment and other personal characteristics and the family relationships of the witness."[260] The evidence shows that WPP coordinators perform this evaluation themselves,[261] rather than relying on psychologists or psychiatrists. Furthermore, the WPP does not have psychologists on staff.

---

257 The House of Commons Standing Committee on Public Safety and National Security called for similar measures in recommending that "…the *Witness Protection Program Act* be amended so that potential candidates are automatically offered the aid of legal counsel with an appropriate security clearance during the negotiation of the candidate's admission to the Witness Protection Program and the signing of the protection contract. The fees of such counsel should be paid by the independent Office responsible for witness protection at the Department of Justice": House of Commons Report on the Witness Protection Program, p. 28.

258 See, for example, Testimony of Geoffrey Frisby, vol. 69, October 30, 2007, p. 8794. See also Testimony of Régis Bonneau, vol. 77, November 16, 2007, pp. 9764-9765.

259 Testimony of Yvon Dandurand, vol. 68, October 29, 2007, pp. 8681-8682.

260 *Witness Protection Program Act*, s. 7(e).

261 Testimony of Raf Souccar, vol. 70, October 31, 2007, p. 8915. Former WPP Coordinator Geoffrey Frisby testified that he would generally conduct these assessments himself, but that he had access to a psychologist when required: Testimony of Geoffrey Frisby, vol. 69, October 30, 2007, p. 8800.

The House of Commons Standing Committee on Public Safety and National Security recommended in its March 2008 report that the WPPA be amended to require an automatic psychological assessment of candidates over the age of 18, including family members, before any candidate is admitted to the WPP, particularly when a change of identity is being considered.[262]

This recommendation makes sense. In terrorism investigations and prosecutions, psychological evaluations could help the National Security Witness Protection Coordinator make decisions about admitting individuals into the witness protection program. Evaluations could also help to ensure that protective measures are tailored to individual needs. However, evaluations can also constitute relevant material that may have to be disclosed to the accused if it relates to the testimony of the witness and is not in an exempt category.

8.6.8.4 Witnesses who are Minors

To date, all minors who have entered the WPP have done so as family members of an adult protectee. The adult protectee signs the protection agreement for children who are admitted. However, the current WPP admission process and RCMP policies make no provision for minors who enter the WPP as individual protectees. While this situation has yet to arise, there may come a time when a key witness in a terrorism case will be a minor who needs protection.

Dandurand told the Commission that the issue of minors as individual protectees has been given very little thought both in Canada and abroad. He suggested that this is in large part because the major drug and organized crime cases that have been at the root of most developments in witness protection do not usually involve witnesses who are minors. However, he said, terrorism investigations and prosecutions are more likely to involve minors.[263] For example, four of the original alleged co-conspirators in the ongoing "Toronto 18" terrorism prosecution[264] were minors, as is the one person who had been convicted at the time of writing. Informers with information about accused who are minors may well come from that same age group. In addition, an alleged conspirator who is a minor might choose to testify against associates. In such cases, the minors might need witness protection.

If a minor decided to help authorities to investigate members of the minor's family, possibly even the parents, the parents could not be expected to act in the best interests of the minor in witness protection matters. It would then be necessary to have in place a process that would enable some authority other than the parents to make decisions on behalf of the minor.

If a minor becomes a witness in a terrorism case, other issues arise:

---

262 House of Commons Report on the Witness Protection Program, p. 27.
263 Testimony of Yvon Dandurand, vol. 69, October 30, 2007, pp. 8701-8702.
264 *R. v. N.Y.*, unreported decision, September 25, 2008 (Ontario Sup. Ct.) Court File YC-07-1587.

- whether a minor can decide alone to cooperate with the authorities and enter the WPP, or whether a minor's guardian(s), or even youth services agencies, could prevent the minor from entering the WPP (or whether they could force the minor to enter the WPP); and
- how to deal with possible variations among provincial youth protection statutes that might in turn impose differing requirements on handling witnesses who are minors.

Several witnesses before the Commission called for an examination of methods of dealing with witnesses who are minors.[265] As recommended above, the National Security Witness Protection Coordinator would be responsible for strategic direction and policy advice to guide CSIS, police forces, Crown prosecutors and the WPP when handling witnesses who are minors. The Coordinator should be able to consult with relevant officials, including provincial child welfare authorities, on these matters.

8.6.8.5 Collaborators who are Inmates

Some protectees acquired their knowledge of targeted organizations while participating in the illegal activities of those organizations. They are criminals themselves and are described here as "collaborators." Because of their criminal activities, these collaborators may be facing or serving jail sentences. If sentenced to imprisonment of two years or more, imprisoned collaborators ("collaborator inmates") serve their sentence under the supervision of the Correctional Service of Canada (CSC).

The Commission heard evidence that collaborator inmates who testify against their organizations are generally despised by other inmates. There is a very real risk that they will be seriously harmed or killed in prison.[266] Pierre Sangollo, CSC Director of Intelligence and National Project Manager, Public Safety, suggested that collaborators can face an even greater risk if they testify against an international terrorist organization because inmates sympathetic to the organization's cause, but whose sympathies are unknown to the collaborator, might target the collaborator.[267]

The evidence before the Commission shows that the odds of a collaborator remaining anonymous during incarceration are extremely remote.[268] This, coupled with the apparently greater risk of retaliation in terrorism cases, creates a very dangerous situation for collaborator inmates connected with such cases.

Protecting collaborator inmates by using administrative segregation to isolate them from the general population is the general practice today.[269]

---

265 See, for example, Testimony of Yvon Dandurand, vol. 69, October 30, 2007, p. 8701. See also Testimony of Anne-Marie Boisvert, vol. 69, October 30, 2007, pp. 8776-8777.

266 Testimony of Pierre Sangollo, vol. 77, November 16, 2007, p. 9835. See also Testimony of Michael Bettman, vol. 77, November 16, 2007, pp. 9842-9843.

267 Testimony of Pierre Sangollo, vol. 77, November 16, 2007, p. 9824.

268 Testimony of Pierre Sangollo, vol. 77, November 16, 2007, p. 9834.

269 Testimony of Pierre Sangollo, vol. 77, November 16, 2007, p. 9869; Testimony of Michael Bettman, vol. 77, November 17, 2007, pp. 9829, 9838.

CSC's objective is to find the least restrictive environment for collaborator inmates. Inmates in less restrictive environments have better access to programs, employment and education and can "move forward" in their correctional plans.[270] However, once anonymity is no longer possible, segregation is the only way to ensure protection for collaborator inmates.[271] Because of the high likelihood of being exposed, collaborators are likely to go directly from a segregation unit in the reception centre to one in a penitentiary. The evidence before the Commission clearly shows that, because of their frequent need for segregation, collaborators as a whole endure poorer conditions than those in the general inmate population.[272]

In some cases, collaborators testify before they are tried for the offences they may have committed. In such cases, collaborators are detained in local provincial facilities before testifying[273] and become the CSC's responsibility only when convicted. However, Sangollo noted that collaborators increasingly plead guilty and are sentenced before they testify. In this way, they may fall under the CSC's jurisdiction (if sentenced to two years or more) and receive protection from the CSC much earlier than would otherwise be the case. As a result, besides protecting those who have already testified, the CSC frequently needs to protect those who have yet to testify. Sangollo told the Commission that this places considerable strain on CSC resources and programs.[274] Furthermore, since the Crown will want access to its witness during the pre-trial and trial phases, moving the collaborator inmate to another region or province is impossible. Terrorism trials may be lengthy,[275] and a collaborator inmate may have to wait years to testify. During that time, the CSC will be unable to move the inmate to a "less restrictive environment," leaving the inmate in segregation.

The unfortunate result is that an important terrorism witness is likely to be held in segregation at the very time that the police and Crown need the full cooperation of the witness. This seems to be a recipe for serious problems. Collaborators who are isolated and unable to participate in prison programs might simply refuse to cooperate further. In most cases, the collaborator inmate will already have pleaded guilty and been sentenced, so there is nothing more for the inmate to lose and much to gain by ceasing to cooperate. Souccar reinforced this point when he told the Commission that an individual has little incentive to assist law enforcement if he or she is disadvantaged by providing that assistance.[276] Boisvert told the Commission that a perception that the worst

---

270 Testimony of Michael Bettman, vol. 77, November 16, 2007, p. 9844.

271 Testimony of Pierre Sangollo, vol. 77, November 16, 2007, pp. 9836-9837. This view is shared by Michael Bettman: Testimony of Michael Bettman, vol. 77, November 16, 2007, p. 9838.

272 For example, Dandurand told the Commission that collaborators often need to serve their whole sentence in isolation and in very difficult circumstances, particularly in psychological terms: Testimony of Yvon Dandurand, vol. 68, October 29, 2007, p. 8689. Boisvert told the Commission that the net result was for collaborator inmates to be systematically treated more harshly than those they help to convict: Testimony of Anne-Marie Boisvert, vol. 69, October 30, 2007, p. 8767.

273 Testimony of Pierre Sangollo, vol. 77, November 16, 2007, pp. 9819-9820.

274 Testimony of Pierre Sangollo, vol. 77, November 16, 2007, pp. 9820-9821.

275 For more on this topic, see Chapter IX.

276 Testimony of Raf Souccar, vol. 71, November 1, 2007, pp. 8953-8954. This point was conceded by the Attorney General of Canada: Final Submissions of the Attorney General of Canada, Vol. III, para. 195: "With respect to witnesses in detention, it is submitted that the harsh detention conditions they may face are a disincentive to cooperation."

treatment awaits those who cooperate will doom the system to failure in the long term.[277]

Because of the importance of collaborator inmates in terrorism investigations and prosecutions, great care is required to avoid discouraging them from helping the authorities. Witnesses before the Commission proposed a variety of ways to prevent alienating collaborator inmates by improving their detention conditions. These included the following:

- transferring collaborator inmates to other Canadian penitentiaries or facilities in other countries;
- building a penitentiary or adequate facility for the exclusive use of collaborator inmates;
- creating a special wing within a larger penitentiary for collaborator inmates;
- creating a special unit in the middle of a military base; and
- transporting collaborator inmates away from the penitentiary for rehabilitation programs.[278]

Collaborators clearly deserve treatment that, to the extent possible given their security needs, is comparable to that given other inmates. They also need the same chances to obtain release under parole. At the same time, it is important to avoid giving collaborators preferential treatment, since this could be seen as "buying" their testimony and might affect their credibility as witnesses.

Given the range of possible solutions, the complexity of the collaborator inmate issue and the number of agencies that have an interest in the issue, some have called for an interdepartmental committee to consider protection options.[279] Certainly, federal agencies such as the CSC, the Attorney General of Canada, Immigration Canada, the RCMP and CSIS would wish to take part. The National Security Witness Protection Coordinator could help to air and resolve the concerns of these bodies and of collaborator inmates.

8.6.8.6 Investigative Hearings

The *Criminal Code* was amended in 2001 to allow investigative hearings in connection with "an investigation of a terrorism offence."[280] The investigative hearing provision lapsed in 2007 as the result of a five-year "sunset clause"[281] in

---

277 Testimony of Anne-Marie Boisvert, vol. 69, October 30, 2007, p. 8769.

278 Testimony of Pierre Sangollo, vol. 77, November 16, 2007, p. 9864. See also Testimony of Michael Bettman, vol. 77, November 16, 2007, pp. 9844-9845, 9878.

279 Testimony of Pierre Sangollo, vol. 77, November 16, 2007, pp. 9864-9865. The Attorney General of Canada favoured creating an interdepartmental committee, arguing that the committee could consider various options, including the international relocation of detained collaborators: Final Submissions of the Attorney General of Canada, Vol. III, para. 195. No other parties or intervenors made submissions about protecting collaborator inmates.

280 *Criminal Code*, s. 83.28(2).

281 *Criminal Code*, s. 83.32.

the *Anti-terrorism Act*.[282] Bill S-3, introduced on March 7, 2008, proposed to re-introduce these investigative hearings in the *Criminal Code*.[283] The Bill died on the Order Paper with the calling of the October 2008 federal election, but was revived in the House of Commons as Bill C-19 on March 12, 2009.[284]

Under the *Criminal Code* provision, a peace officer, with the consent of the Attorney General of Canada or a provincial Attorney General, could apply to a judge for an order for the gathering of information from a named individual. If the judge decided to hold a hearing, the judge would have the power to compel a person to testify. Section 83.29 of the *Criminal Code* provided for means to compel the attendance and cooperation of the person.

The only attempt to use investigative hearings occurred during the Air India trial, where the Supreme Court of Canada upheld their constitutionality.[285] The Court also stated that because investigative hearings are judicial hearings, there is a presumption that they will be held in open court.[286]

Witnesses who are compelled to appear before investigative hearings are likely to face the same threats, intimidation and retaliation as witnesses who testify in criminal trials or otherwise assist the authorities. It seems unlikely that a terrorist organization would view the compelled testimony of a witness at an investigative hearing any more charitably than it would view their testimony at trial. In his research paper, Dandurand was skeptical of claims that compelled witnesses would be insulated from threats and retaliation simply because they were compelled to cooperate. [287] He reinforced this point in his testimony.[288]

RCMP Superintendent Michel Aubin testified that the police could seek admission to the WPP for individuals who have been compelled to testify at investigative hearings.[289] In addition, he said, the RCMP might conduct a threat assessment at that point.[290] Souccar confirmed that the RCMP would be as proactive in identifying threats to compelled witnesses as it would be with other witnesses. He testified that RCMP investigators generally "…have a good sense of the individuals being investigated" and that "…should it be that the individual subject to the investigative hearing could potentially be at risk," the investigators would "…get ahead of the ball, ahead of the curve and either notify the individual [or] put measures in place." Souccar did not exclude the possibility that the RCMP might perform a formal threat assessment for the witness, should the situation warrant one.[291]

---

282 S.C. 2001, c. 41.
283 *An Act to amend the Criminal Code (investigative hearing and recognizance with conditions)*, 2nd Sess., 39th Parl., 2007-2008.
284 *An Act to amend the Criminal Code (investigative hearing and recognizance with conditions*), 2nd Sess., 40th Parl., 2009.
285 *Application under s. 83.28 of the Criminal Code (Re)*, 2004 SCC 42, [2004] 2 S.C.R. 248.
286 *Re Vancouver Sun* 2004 SCC 43, [2004] 2 S.C.R. 332.
287 Dandurand Paper on Protecting Witnesses, p. 43.
288 Testimony of Yvon Dandurand, vol. 69, October 30, 2007, p. 8698.
289 Testimony of Michel Aubin, vol. 70, October 31, 2007, p. 8939.
290 Testimony of Michel Aubin, vol. 70, October 31, 2007, p. 8940.
291 Testimony of Raf Souccar, vol. 70, October 31, 2007, pp. 8940-8941.

Witnesses forced to appear before investigative hearings would appear to satisfy the broad definition of "witness" in section 2 of the WPPA, and therefore could presumably enter the WPP if a police force recommends entry. Under the proposals discussed earlier, the National Security Witness Protection Coordinator would advise about witness protection matters in investigative hearings. This could include considering any damage that compelling testimony might cause to the fragile trust between some communities and police and intelligence agencies. The Coordinator should also consider which protection measures could be used in a given investigative hearing when the witness may be inadvertently or deliberately identified to the public or the affected parties. This would avoid the present conflict of interest encountered by the RCMP. The RCMP, as the investigating force, may have an interest in conducting an investigative hearing to obtain information and evidence. It will also be in charge of determining whether the witness who is being compelled to testify in what may be a public hearing also needs witness protection.

The now-defunct investigative hearing provisions did not explicitly provide for the Crown or police to assess threats to compelled witnesses, nor does Bill C-19 impose such an obligation. As well, RCMP policy does not require a threat assessment for witnesses forced to appear before investigative hearings.

Investigative hearings are contentious, in part because they place an onerous obligation on the ordinary citizen. Dandurand stressed that the police must take immediate steps to ensure the protection of any witnesses asked or compelled to testify.[292] The authorities should fully explore less public and less coercive means to secure information from a person with information relevant to a terrorism investigation. An investigative hearing not only forces a reluctant human source to cooperate, but it also runs a real risk of disclosing that source's identity.

If investigative hearings are revived and if they are deemed to be necessary in a particular investigation, the RCMP is the police force most likely to apply for such hearings, and an Attorney General must support the requests. Both have at least an ethical obligation to ensure that appropriate protection measures are in place or available to those who are forced to provide information at an investigative hearing. They should also carefully consider the possibility that a person compelled to testify at an investigative hearing may later turn out to be a person who could be charged with a terrorism offence. Once the person has been compelled to testify at an investigative hearing, the state cannot use the compelled material or any material derived from that material against the person in subsequent proceedings.[293]

Under the Commission's proposals, the National Security Witness Protection Coordinator should be responsible for deciding whether witness protection was necessary for the subject of an investigative hearing.

---

292 Testimony of Yvon Dandurand, vol. 69, October 30, 2007, pp. 8698-8699.

293 *Application under s. 83.28 of the Criminal Code (Re)*, 2004 SCC 42, [2004] 2 S.C.R. 248 at paras. 71-72.

8.7 Conclusion

This chapter has described how, through threats and violence, including murder, extremists deter individuals from assisting police and intelligence agencies in terrorism investigations and prosecutions. Intimidation also discourages others from coming forward to help. The examples of intimidation relating to the investigation of the Air India tragedy showed clearly that too many individuals who assisted the state as witnesses and sources, or even merely spoke out against extremism, suffered unnecessary hardship. That is a deterrent, not an incentive, for others to volunteer, and a clear indication that witness protection needs were not being met. The Air India case also showed how community-wide intimidation can breed a dangerous silence among those best positioned to help investigate and prosecute terrorists.

The chapter has examined ways to reduce the potential danger to individuals who assist the authorities. Keeping the identity of such individuals completely secret can be achieved through a variety of mechanisms, including the police informer privilege or a non-disclosure order made under sections 37 or 38 of the *Canada Evidence Act*. Nevertheless, anonymity of sources, let alone witnesses, is not always possible if criminal prosecutions for terrorism offences proceed. In such cases, other measures – both legal and operational – can reduce the risk to witnesses and sources and help foster their willingness, and that of their communities, to help authorities. A range of partial anonymity alternatives between full disclosure and total anonymity may also reduce the risks that witnesses may face. These include the use of closed courts, publication bans, screens, videotaped testimony and testifying under a pseudonym.

Judges, like other justice system participants, need to understand the difficulties faced by some witnesses and sources. Judges should not hesitate to devise creative and reasonable solutions which can reconcile the demand for public disclosure on the one hand and the secrecy that may be necessary to protect witnesses and encourage potential witnesses, on the other.

The Witness Protection Program represents the most forceful response to threats against witnesses and sources. However, despite its excellent record in safeguarding the lives of protectees, the current Program is not fully attuned to the needs of sources and witnesses in terrorism investigations and prosecutions.

It is essential to have a flexible witness protection program that allows the precise level and method of protection to be tailored to the particular circumstances and needs of the protectee. This chapter discussed several ways to improve the current Program and to mitigate the difficulties that flow from entering the Program. These include the acquisition of a better understanding of the nature and needs of protectees in terrorism matters and the introduction of a process for making decisions about witness protection which is independent of the interests of police and prosecutors and which more closely reflects the interests of witnesses themselves.

A key element of witness protection reform is the proposed National Security Witness Protection Coordinator. The creation of this position would remove the administration of witness protection from the RCMP and prosecutors.

Even if a witness protection program becomes more closely attuned to the needs of witnesses and sources, entering the program can painfully disrupt the lives of protectees and of those around them. The best-designed and most humane witness protection programs cannot avoid imposing this hardship. For this reason, the human dimension of witness protection must always figure prominently in decisions about how and when to use witnesses and sources in terrorism investigations and prosecutions.

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

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

9.0 Introduction

The Commission's terms of reference require the Commissioner to make findings and recommendations about "…whether the unique challenges presented by the prosecution of terrorism cases, as revealed by the prosecutions in the Air India matter, are adequately addressed by existing practices or legislation." They also specifically ask what "changes in practice or legislation" are required to address the challenges of terrorism prosecutions, "…including whether there is merit in having terrorism cases heard by a panel of three judges."[1]

The "prosecutions in the Air India matter" refer to the prosecutions of Ripudaman Singh Malik ("Malik"), Ajaib Singh Bagri ("Bagri") and Inderjit Singh Reyat ("Reyat") in the British Columbia Supreme Court.[2] These prosecutions resulted in the longest and most expensive trial in Canadian history, referred to here as the "Air India trial."

This chapter examines the challenges facing terrorism trials as illustrated by the experience of the Air India trial. It first recounts the trial in some detail. This is done not to second-guess the verdict but rather to make clear the many challenges of terrorism prosecutions. It is important that Canadians understand the extraordinary measures that were taken to conduct this trial and to have it reach a verdict. Such measures will not be duplicated easily in the future.

Terrorism prosecutions require reform to make them manageable. This chapter discusses how to respond to the challenges of voluminous disclosure, multiple pre-trial motions and trial by jury in terrorism prosecutions. It also examines whether there is merit in having terrorism trials heard by a panel of three judges.

---

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

2 As referred to in the indictment filed on June 5, 2001, which charged Malik, Bagri and Reyat jointly.

In recent years, several reports have called for better management of complex criminal trials – the so-called "mega-trials" or "mega-cases." These typically involve multiple accused charged with multiple offences. They are also characterized by extensive disclosure obligations and multiple pre-trial motions.[3] Most terrorism trials will exhibit the characteristics of a mega-trial, as did the Air India trial.

There is no need to repeat much of the valuable research already done on the challenges of the mega-trial. For example, the Barreau du Québec produced a report in 2004,[4] as did the Steering Committee on Justice Efficiencies and Access to the Criminal Justice System.[5] The Ontario Chief Justice's Advisory Committee on Criminal Trials in the Superior Court of Justice produced a report in 2006.[6] In the autumn of 2008, the Federal/Provincial/Territorial Working Group on Criminal Procedure issued proposals for reform of mega-trials after it heard from a roundtable of experts.[7] Most recently, the Hon. Patrick LeSage, Q.C., and Professor (now Justice) Michael Code issued a report to the Attorney General of Ontario on large and complex criminal case procedures.[8]

All these reports are valuable, but they do not focus on the specific challenges facing terrorism trials.[9] Solutions designed for mega-trials in general may not be suitable for terrorism prosecutions, in part because terrorism prosecutions will almost inevitably involve deciding whether secret intelligence must be disclosed to the accused. In addition, terrorism prosecutions may be more resistant to

3 There appears to be no accepted definition of what constitutes a "mega-trial" or "mega-case." However, the Steering Committee on Justice Efficiencies and Access to the Criminal Justice System provided a workable definition, calling it "...a trial with such complex evidence or a number of accused such that one or both of these characteristics result in exceptionally long proceedings": Department of Justice Canada, *Final Report on Mega trials of the Steering Committee on Justice Efficiencies and Access to the Criminal Justice System to the F/P/T Deputy Ministers Responsible for Justice* (2004), p. 2, online: Department of Justice Canada <http://www.justice.gc.ca/eng/esc-cde/mega.pdf> (accessed December 4, 2008) [Steering Committee Report on Mega trials].

4 Exhibit P-370: Ad Hoc Committee of the Criminal Law Committee on Mega-trials, *Final Report* (February 2004) [Barreau Report on Mega-trials].

5 Steering Committee Report on Mega trials.

6 Superior Court of Justice (Ontario), *New Approaches to Criminal Trials: The Report of the Chief Justice's Advisory Committee on Criminal Trials in the Superior Court of Justice* (May 12, 2006), online: Ontario Courts <http://www.ontariocourts.on.ca/sjc/en/reports/ctr/index.htm> (accessed December 1, 2008) [Ontario Superior Court Report on Criminal Trials].

7 Federal/Provincial/Territorial Working Group on Criminal Procedure, *Proposals for Reform: Mega-Trials* (2008) [F/P/T Working Group Proposals on Mega-Trials]. See also, for example, Michael Code, "Law Reform Initiatives Relating to the Mega Trial Phenomenon" (2008) 53 Crim. L.Q. 421 [Code Article on Mega Trial Phenomenon].

8 Patrick Lesage and Michael Code, *Report of the Review of Large and Complex Criminal Case Procedures* (November 2008), online: Ontario Ministry of the Attorney General <http://www.attorneygeneral.jus.gov.on.ca/english/about/pubs/lesage_code/lesage_code_report_en.pdf> (accessed December 5, 2008) [Lesage and Code Report on Large and Complex Criminal Case Procedures].

9 But see Lesage and Code Report on Large and Complex Criminal Case Procedures for some discussion of the unique challenges of terrorism prosecutions and their recommendation at p. 93 that Ministers of Justice consider modifications to the procedure under s. 38 of the *Canada Evidence Act* "in order to eliminate the delays caused in major terrorism prosecutions by the bifurcation of the case and by interlocutory appeals". Similar recommendations are made by the Commission in Chapter VII.

plea discussions and guilty pleas than would mega-trials involving organized crime. Finally, because terrorism prosecutions involve national security matters, the federal interest in such trials is greater than in other mega-trials.

To assist the Commission with issues relating to terrorism prosecutions, Professor Bruce MacFarlane prepared a paper on structural aspects of terrorism trials. This paper included an examination of the possible merit in having terrorism trials heard by a three-judge panel.[10] Professor Robert Chesney prepared a paper on the extensive post- 9/11 American experience with terrorism prosecutions.[11] Professor Kent Roach prepared a paper on the unique challenges of terrorism prosecutions, focusing on developing a workable relation between intelligence and evidence.[12] Commission counsel prepared a background document on the management of terrorist mega-trials.[13] In addition, several witnesses, including lawyers from the Air India trial, testified about the challenges of terrorism prosecutions. The Commission was also able to review a "lessons learned" account of the Air India trial prepared by Robert Wright, Q.C., the lead prosecutor in the case, and Michael Code, one of the defence counsel.[14]

A failure to reform the trial process to address the many challenges of terrorism prosecutions will make it more difficult to prevent terrorism and punish terrorists in Canada through prosecutions. Canada has less experience than many of its allies with terrorism prosecutions. In the 1980s, a number of terrorism prosecutions, including one against Talwinder Singh Parmar and another involving an alleged conspiracy to blow up an Air India aircraft in 1986, collapsed because of problems arising from the disclosure of information that would identify informers. Another terrorism prosecution was abandoned after the disclosure of an affidavit used to obtain a CSIS wiretap warrant. A mistrial was declared in one prosecution after Federal Court litigation about whether the accused could call secret information in his defence.[15] There have been a few post-9/11 terrorism prosecutions, including two that led to convictions in 2008: that of a young offender in relation to an alleged 2006 Toronto plot and that of Mohammad Momin Khawaja[16] (which led to a guilty verdict) in relation to an international terrorist plot. Nevertheless, Canada has had much less experience with terrorism prosecutions than the United Kingdom or the United States.[17]

---

10 Bruce MacFarlane, "Structural Aspects of Terrorist Mega-Trials: A Comparative Analysis" in Vol. 3 of Research Studies: Terrorism Prosecutions, pp. 246-261 [MacFarlane Paper on Terrorist Mega-Trials].

11 Robert M. Chesney, "Terrorism and Criminal Prosecutions in the United States" in Vol. 3 of Research Studies: Terrorism Prosecutions [Chesney Paper on Terrorism and Criminal Prosecutions].

12 Kent Roach, "The Unique Challenges of Terrorism Prosecutions: Towards a Workable Relation Between Intelligence and Evidence" in Vol. 4 of Research Studies: The Unique Challenges of Terrorism Prosecutions [Roach Paper on Terrorism Prosecutions].

13 Exhibit P-300: Background Dossier For Term of Reference (b)(vi): "The Management of Terrorist Mega-trials" [Background Dossier For Term of Reference (b)(vi)].

14 Exhibit P-332: Robert Wright and Michael Code, "Air India Trial: Lessons Learned" [Wright and Code Report on Air India Trial].

15 For extensive case studies of these and other terrorism prosecutions and prosecutions involving national security, see Roach Paper on Terrorism Prosecutions.

16 *R. v. Khawaja*, [2008] O.J. No. 4244 (Sup. Ct.).

17 Roach Paper on Terrorism Prosecutions, p. 48.

Canada will continue to lag behind its allies in its ability to conduct fair and efficient terrorism prosecutions unless some fundamental reforms are made.

In his 2005 report, the Hon. Bob Rae described the Air India trial as "…long and complex, the most expensive and difficult in the history of the country."[18] The length and complexity of the trial, plus national security concerns about disclosure of some evidence, created a series of obstacles that do not typically arise in criminal cases. These obstacles, had they not been addressed effectively, could have prevented the reaching of a verdict or caused the case to, as MacFarlane describes it, "collapse under [its] own weight."[19]

MacFarlane summarized the challenges associated with terrorism trials when he testified before the Commission:

> [T]he real problem, in my view, relates to length primarily, complexity secondarily, and the risk of not being able to reach verdict in a lengthy terrorist trial. And it appears that most of the terrorist trials that have arisen in Canada are expected to be lengthy and have been lengthy. So it's not an idle concern.[20]

Later, he spoke of the urgent need for reform:

> There are so many impediments to completing a mega-trial in Canada -- so many points at which the presiding judge may decide to enter a judicial stay or the Crown might have to enter a Crown stay. There are so many roadblocks particularly in relation to the jury on a mega-trial that I am greatly fearful that Canada is not able to run lengthy terrorist cases. I greatly fear that we are not -- we don't have the tools to run these trials. That will not bode well if our trials consistently fail, case after case after case. And [I] greatly fear that some of the cases, that we are either looking at right now or will be looking at in the not-too-distant future, will fail, and Canada will be seen as a place where the criminal justice system simply can't cope with significant terrorist acts that result in a mega-trial. For that reason, it seems to me that maintaining the status quo is simply not an option. We need a rethinking of our approach to these mega-trials because I do feel that most of the terrorist trials that will arise and have arisen in Canada will be mega-trials. So we're right into it right now.[21]

---

18 *Lessons to be Learned: The report of the Honourable Bob Rae, Independent Advisor to the Minister of Public Safety and Emergency Preparedness, on outstanding questions with respect to the bombing of Air India Flight 182* (Ottawa: Air India Review Secretariat, 2005), p. 24 [*Lessons to be Learned*].

19 MacFarlane Paper on Terrorist Mega-Trials, p. 159.

20 Testimony of Bruce MacFarlane, vol. 79, November 20, 2007, p. 10068.

21 Testimony of Bruce MacFarlane, vol. 79, November 20, 2007, p. 10074.

In his report for the Commission, MacFarlane identified three overarching challenges for future terrorism trials:

> [F]irst, they need to be manageable in terms of length and complexity. Second, the process and result need to be seen as fair and legitimate, both domestically and in the eyes of the international community. Finally, any new criminal trial process cannot increase the risk of convicting persons who are innocent of the crimes charged.[22]

He also posed questions at the core of the search to meet these goals:

> Should the institutional underpinning or "structural" elements of the trial process in Canada be changed to meet the tremendous challenges posed by terrorist trials? Can we provide trials for accused terrorists that comport with Canadian standards of justice, notwithstanding the complex challenges inherent when national security is at risk?[23]

In his report for the Commission, Roach stressed the need for just and efficient processes that respect the principles of fairness to the accused and openness of proceedings, but that also respect important interests in the protection of legitimate secrets developed by Canada's intelligence agencies and its foreign counterparts.[24] Chapter VII discussed Canada's present system, which requires issues of national security confidentiality to be litigated in the Federal Court, with the matter then returning to the trial court. This can fragment and delay terrorism prosecutions and deprive the trial judge of the power to manage the disclosure of secret information and other pre-trial matters.

An important theme in this chapter is the need for the trial judge to be in charge of all aspects of the terrorism prosecution in order to ensure the efficiency and the fairness of the process. The chapter examines several issues relating to terrorism trials: voluminous disclosure, multiple pre-trial motions, control by judges of court proceedings and counsel, securing adequate defence representation, ensuring the viability of juries, federal-provincial cost-sharing to support lengthy trials, and providing for the needs of victims and witnesses. Those issues that can be resolved at the federal level are addressed.

Although some issues relating to terrorism prosecutions fall under provincial jurisdiction, the federal government has an important role in prosecutions that affect national security. As discussed in Chapter III, the Attorney General of Canada can prosecute cases involving terrorism offences and other conduct that affects national security.

---

22 MacFarlane Paper on Terrorist Mega-Trials, p. 235.
23 MacFarlane Paper on Terrorist Mega-Trials, p. 159.
24 Roach Paper on Terrorism Prosecutions, pp. 91-93.

9.1 The Challenges of Terrorism Prosecutions

Terrorism prosecutions are difficult – in part because they often involve multiple accused, multiple charges and voluminous disclosure. Criminal trials such as those involving organized crime may also exhibit these features, but they will not involve the same issues as terrorism trials concerning the disclosure of intelligence.

The challenges of terrorism prosecutions can be addressed by reforms such as using severance more often to produce smaller, more manageable prosecutions, avoiding overloaded indictments and using electronic disclosure. However, terrorism trials may be more complex and longer than other trials, as MacFarlane testified, because of the need to establish matters surrounding the terrorist act, such as "…planning, deliberation, the execution, [and] how many people were involved; it's the proof that's required to present the picture concerning the developments up to and including the terrorist act."[25] In addition, terrorism prosecutions may require the Crown to establish the existence of a terrorist group in addition to other elements of an offence.

Proving terrorism offences often involves the difficulty of proving "anticipatory" elements of offences – for example, conspiracy, providing or collecting property intending that it be used to carry out a terrorism offence[26] or contributing to any activity of a terrorist group for the purpose of enhancing its ability to facilitate or carry out a terrorist activity.[27] Roach observed that: "The expansion of the criminal law means that what would have been, before 2001, advance intelligence that warns about threats to the security of Canada may, in some cases, now also be evidence of one of the [terrorism] crimes…."[28]

The terrorism offence provisions of the *Criminal Code* involve significant maximum penalties, many of which are to be served consecutively.[29] The prospect of significant penalties may make guilty pleas less likely, and prosecutors may not consider it to be in the public interest to engage in plea bargains which significantly reduce penalties. As a consequence, the accused may not have an incentive to engage in plea discussions, and the number of trials will increase as a result.

In addition, because of the difficulties surrounding the disclosure of secret information to the accused, disclosure issues may not be fully resolved early in the trial process. This also limits the potential for resolving plea negotiations, since the accused might want disclosure issues addressed first. Some accused may have strong ideological beliefs that make them resist the idea of pleading guilty. Prosecutors and defence lawyers may also, for different reasons, be less inclined to begin plea discussions in terrorism cases, placing further strain on the trial process.

---

25 Testimony of Bruce MacFarlane, vol. 78, November 19, 2007, pp. 9892-9896.
26 *Criminal Code*, R.S.C. 1985, c. C-46, s. 83.02 [*Criminal Code*].
27 *Criminal Code*, s. 83.18.
28 Roach Paper on Terrorism Prosecutions, p. 48.
29 *Criminal Code*, s. 83.26.

Most significantly, terrorism trials are likely to have a national security dimension that will involve applications – at present made to the Federal Court under section 38 of the *Canada Evidence Act*[30] – for non-disclosure of information that, if disclosed, will harm national security, national defence or international relations. This raises the prospect of numerous pre-trial motions that would not occur in other criminal trials. Few ordinary criminal trials, even major trials involving organized crime, would involve the potential disclosure of "sensitive information" that would bring section 38 into play.

In his report to the Commission, Professor Roach conducted extensive case studies of terrorism prosecutions in Canada. He concluded that these case studies "…raise doubts about whether Canadian practices and laws are up to the demands of terrorism prosecutions, particularly as they relate to the relation between intelligence and evidence and the protection of informants."[31]

As discussed throughout this volume, the interplay between intelligence and evidence is one of the central and unique features of both terrorism investigations and prosecutions. Earlier chapters have analyzed in considerable detail the relationship between intelligence and evidence and the role of section 38. This chapter therefore does not address section 38 extensively, but does recognize that section 38 applications are likely to be an important matter to be addressed in the management of many terrorism prosecutions. The recently completed *Khawaja* prosecution provides a good example. There, pre-trial motions involving applications for non-disclosure under section 38 were extensively litigated over 18 months in 2007 and 2008.[32] The trial itself took only 27 days.[33] The defence also attempted unsuccessfully to persuade the Supreme Court of Canada to hear an appeal before the trial had even started.[34] Such interlocutory appeals – appeals made before a trial has been completed -- are not permitted in regular criminal prosecutions.

Terrorism trials often have an international dimension, since the planning and execution of terrorist acts may involve players in several countries. This can complicate the trial process in several ways. First, the Crown may need to rely on evidence gathered in, or flowing through, foreign countries; to obtain this evidence requires international cooperation. In some cases, CSIS may already have foreign intelligence that could be useful as evidence or that might be subject to disclosure obligations, but it will need to seek permission from a foreign government to use it for a criminal prosecution. In some cases, foreign intelligence authorities that provided information to Canadian authorities may

---

30 R.S.C. 1985, c. C-5.

31 Roach Paper on Terrorism Prosecutions, pp. 288-289.

32 *Canada (Attorney General) v. Khawaja*, 2007 FC 463, 280 D.L.R. (4th) 32, aff'd 2007 FCA 388, 289 D.L.R. (4th) 260, application for leave to appeal dismissed (2008), 166 C.R.R. (2d) 375 (S.C.C.); *Canada (Attorney General) v. Khawaja*, 2007 FC 490, 219 C.C.C. (3d) 305, allowed in part 2007 FCA 342, 228 C.C.C. (3d) 1; *Canada (Attorney General) v. Khawaja*, 2008 FC 560.

33 *R. v. Khawaja*, [2008] O.J. No. 4244 at para. 2 (Sup. Ct.).

34 See *R. v. Khawaja* (2006), 214 C.C.C. (3d) 399 (Ont. Sup.Ct. J.), application for leave to appeal dismissed 2007 CanLII 11625 (S.C.C.).

not want the information exposed in a prosecution because doing so might compromise ongoing intelligence activities in their country.

The international dimension also raises the possibility of extradition of an accused to Canada to stand trial. Furthermore, where international players must cooperate before a charge can be laid, the pace will ordinarily be determined by the slowest or most reluctant player. This problem may be particularly acute where governments disagree on whether the criminal justice system has a role to play in a particular situation, or whether it should be left to be dealt with exclusively by the intelligence community. Even if they do not involve an international dimension, terrorism trials will often involve several domestic agencies, increasing the possibility that the pace will be determined by the slowest player.

Prosecutors may have difficulties complying with their disclosure obligations, given the volume of material that has to be disclosed. Disclosure may be rendered even more difficult because some relevant material may relate to vulnerable informers, ongoing investigations or material that was provided from a foreign or domestic agency on the understanding that it would not be disclosed. Unfortunately, it is also possible that unethical defence counsel might try to sabotage the trial through prolonged and frivolous motions, including attempts to call or to gain access to secret information that is not relevant to the case.

The offences created by the *Anti-terrorism Act*[35] are very complex and are only starting to be tested. The relative newness of these offences will likely mean that prosecutors will use extra caution in deciding which offences to charge. There may be a tendency, out of an abundance of caution, to lay more charges than might be the case with other, more established, criminal offences. This in turn may lead to longer trials that will test the endurance of judges, jurors, witnesses, victims and lawyers. MacFarlane, for example, warns that the length of some terrorism trials may exhaust juries.[36]

The accused does have a right to a fair trial without unreasonable delay, but this does not mean that the accused has a right to a perfect trial. That said, it will be very important that the justice system treats those accused of terrorism offences fairly to guard against miscarriages of justice.

The cost of terrorism prosecutions may also give rise to disputes between federal and provincial governments. Some provinces may not have the capacity to conduct a prosecution such as the Air India trial. Federal funding may be needed to help with matters such as the construction of secure facilities, payments to defence counsel above normal legal aid rates and the provision of services for victims and the press.

---

35 S.C. 2001, c. 41.

36 MacFarlane Paper on Terrorist Mega-Trials, pp. 251-257.

Terrorism trials involving completed acts of terrorism such as the bombing of Air India Flight 182 may involve many more direct victims than ordinary criminal offences. This will require a much more sophisticated and systematic approach to address the needs of witnesses and victims.

Terrorism is often associated with explosives, and the sheer scale of the forensic investigation (and the resulting evidence) after an explosion is ordinarily much greater than for other violent crimes.

Terrorism trials are also unique because of their public profile. Few criminal trials attract such widespread public interest. In essence, terrorism trials put the justice system on trial in a very public way. MacFarlane argues that accused persons may face the risk of not being able to have a fair trial because of the publicity and pressures that accompany horrific acts of terrorism.[37] However, it is unthinkable that the publicity, cost, complexity or length of a terrorism trial would lead to abandoning a prosecution. As Justice Rutherford said, "The importance of Canada being able to do these things and to make them work without throwing in the towel and saying that we have no capacity to administer criminal justice in cases where national security issues are at stake, cannot be overstated."[38] In short, the fair but efficient conduct of terrorism prosecutions is vital to the national interest.

9.2 The Air India Criminal Trial

On October 27, 2000, Malik and Bagri were each charged with eight counts under the *Criminal Code*. These included the following:

- first degree murder of the 329 Air India Flight 182 passengers and crew;
- first degree murder of the two Japanese baggage handlers who died in the Narita explosion;
- conspiracy to murder the passengers and crew on Air India Flights 182 and 301 and to place bombs likely to endanger safety on board aircraft in service;
- attempted murder of the passengers and crew of Air India Flight 301; and
- causing bombs to be placed on board the various aircraft.[39]

Bagri was also charged with the attempted murder of Tara Singh Hayer, but this indictment was held in abeyance pending the conclusion of the Air India proceedings. The evidence respecting this charge was held not to be admissible in the Air India trial.[40] Malik and Bagri were both detained pending trial and their

---

37 MacFarlane Paper on Terrorist Mega-Trials, p. 293.
38 *R. v. Ribic*, 2004 CanLII 7091 (ON C.A.) at para. 49.
39 See Exhibit D-1: "Background and Summary of the Facts" for more information about the charges.
40 See *HMTQ v. Malik, Bagri and Reyat*, 2002 BCSC 823.

applications for judicial interim release were denied.[41] In July 2002 Bagri made a further application for judicial interim release, citing new delays and changes in the strength of the Crown's case in light of new disclosure and recent pre-trial rulings. His application was denied.[42] Malik and Bagri's first court appearance was October 30, 2000, followed by five days of bail hearings between December 21, 2000, and January 2, 2001.

The Crown preferred direct indictments against Malik and Bagri on March 6, 2001. The trial was scheduled to begin on February 4, 2002, before Justice Ian Josephson, sitting with a jury. According to the schedule discussed during the bail hearing,[43] the review by the defence of the disclosure was to last until the autumn of 2001 and preparation for pre-trial motions would last until the winter of 2002. It was also thought that trial preparation would take five months and that the trial itself would begin in the autumn of 2002. The trial was expected to end by late 2002 or early 2003, but it was understood that possible admissions by the defence and courtroom availability could affect the trial length. In fact, the trial began only in the spring of 2003 and the presentation of evidence concluded in December 2004, nearly two years later than expected. The accused remained in custody throughout.

After the prosecutors obtained consent from the United Kingdom,[44] Reyat was added as a defendant in a new indictment that was filed on June 5, 2001. That indictment charged Malik, Bagri and Reyat jointly for all counts except the murder of the two Narita baggage handlers; Reyat had already been convicted of their manslaughter in 1991.[45] On December 14, 2001, Justice Josephson ruled that Reyat's trial was to proceed jointly with that of the other accused and adjourned the trial to November 1, 2002, despite objections by Malik and Bagri to the joint trial.[46] On April 29, 2002, four of Reyat's counsel withdrew and new

---

41 *Malik and Bagri v. HMTQ*, 2001 BCSC 2; *R. v. Bagri*, 2001 BCCA 273, 45 C.R. (5th) 143 (B.C.C.A.).

42 *Bagri v. R.*, 2002 BCSC 1025.

43 *Malik and Bagri v. HMTQ*, 2001 BCSC 2 at para. 16.

44 The United Kingdom authorized Reyat's extradition on August 10, 1988, to allow him to be tried for his role in the Narita bombing, although he was not actually extradited until December 13, 1989. A condition of the extradition was that the United Kingdom's consent would be required for any further accusations against Reyat. On January 26, 2001, Canada asked the United Kingdom for consent to try him for the Air India bombing: *R. v. Malik, Bagri and Reyat*, 2002 BCSC 1679 at para. 4. This consent was obtained on June 4, 2001 and Reyat was added as a defendant in a new indictment.

45 *R. v. Reyat*, 1991 CanLII 1371 (BC S.C.). This case lasted roughly 18 months (from December 1989 to May 1991). Reyat was charged only with the manslaughter of the two Narita baggage handlers. He was found guilty of both counts and was sentenced to 10 years in prison (the sentencing decision was not reported). Justice Paris concluded, "For all the above reasons I am satisfied beyond a reasonable doubt that the accused either fabricated or, at the very least, aided others in the fabrication of the bomb which exploded in Narita killing the two baggage handlers. The Crown does not argue that it has proved his exact purpose beyond a reasonable doubt but I am satisfied beyond a reasonable doubt that he knew the bomb was to be used for some illicit purpose. It could not be otherwise. According to the *Criminal Code* the elements of manslaughter are directly or indirectly causing the death of a human being by means of an unlawful act." Reyat's 1991 trial was significantly simpler than the Air India trial, since Reyat's trial involved no conspiracy counts and relied on forensic evidence linking Reyat directly with the parts used to create the bomb that killed the two victims. The trial also relied on an admission by Reyat that he constructed the bomb. Reyat's appeal was dismissed by the British Columbia Court of Appeal: *R. v. Reyat* (1993), 80 C.C.C.(3d) 210 (B.C.C.A.).

46 *HMTQ v. Malik, Bagri and Reyat*, 2001 BCSC 1758.

counsel were retained, resulting in a further adjournment of the trial until March 31, 2003.[47]

Because the Crown elected to proceed by direct indictment, no preliminary inquiry occurred.[48] After initial rulings in January 2002 about the scheduling of motions and the scope of the publication ban,[49] the pre-trial motions proceeded between February and December 2002.[50] Thirteen published pre-trial rulings resulted from four Crown motions,[51] four by Bagri,[52] four by Reyat[53] and one motion by all three accused.[54] In addition, media representatives applied for leave to publish information about one of the pre-trial *voir dires*[55] after their general motion to limit the publication ban was denied.[56] Pre-trial motions addressed a wide range of issues, including disclosure, destruction of evidence, admissibility and use of hearsay evidence, editing of evidence, the voluntary nature of statements made by the accused, and alleged *Charter* violations regarding search and seizure and statements obtained from the accused. Almost all the pre-trial applications were heard by Justice Josephson. Other judges heard other applications – for instance, relating to funding of defence counsel[57] and the sentencing of Reyat.[58] No pre-trial motions, however, involved litigation in the Federal Court under section 38 of the *Canada Evidence Act*.

On February 10, 2003, Reyat pleaded guilty to the manslaughter of the Air India Flight 182 victims and the Crown withdrew the other charges against him. He was sentenced to five years in addition to the ten years he had received in 1991 for the manslaughter of the two Narita baggage handlers.[59] On February 24, 2003, Malik and Bagri re-elected, with the Crown's consent, to be tried by judge alone.[60]

The trial began on April 28, 2003, and continued until December 3, 2004, with adjournments during the summer breaks in both 2003 and 2004. The trial lasted a total of 217 trial days.

---

47 See *In the Matter of an Application Under s. 83.28 of the Criminal Code and Satnam Kaur Reyat*, 2003 BCSC 1152 at para. 19.
48 Background Dossier For Term of Reference (b)(vi), p. 96.
49 See *R. v. Malik, Bagri and Reyat*, 2002 BCSC 78; *R. v. Malik, Bagri and Reyat*, 2002 BCSC 80.
50 Background Dossier For Term of Reference (b)(vi), p. 105.
51 *HMTQ v. Malik, Bagri & Reyat*, 2002 BCSC 362; *HMTQ v. Malik, Bagri and Reyat*, 2002 BCSC 823; *R. v. Malik, Bagri & Reyat*, 2002 BCSC 1291; *R. v. Malik, Bagri and Reyat*, 2003 BCSC 29.
52 *R. v. Malik, Bagri and Reyat*, 2002 BCSC 484; *HMTQ v. Malik, Bagri and Reyat*, 2002 BCSC 837; *R. v. Malik, Bagri and Reyat*, 2002 BCSC 864; *R. v. Malik, Bagri and Reyat*, 2003 BCSC 231.
53 *R. v. Malik, Bagri and Reyat*, 2002 BCSC 477; *R. v. Malik, Bagri and Reyat*, 2002 BCSC 1679; *R. v. Malik, Bagri and Reyat*, 2002 BCSC 1731; *R. v. Malik, Bagri and Reyat*, 2003 BCSC 30.
54 *R. v. Malik, Bagri and Reyat*, 2002 BCSC 1427.
55 *R. v. Malik, Bagri and Reyat*, 2002 BCSC 861.
56 *R. v. Malik, Bagri and Reyat*, 2002 BCSC 80.
57 *HMTQ v. Malik*, 2003 BCSC 1439, 111 C.R.R. (2d) 40 at para. 3.
58 *R. v. Reyat*, 2003 BCSC 254.
59 *R. v. Reyat*, 2003 BCSC 1152.
60 See the procedural history in *Application under s. 83.28 of the Criminal Code (Re)*, 2004 SCC 42, [2004] 2 S.C.R. 248 at para. 14.

The trial took place in Courtroom 20, a very secure, state-of-the-art electronic courtroom specially renovated for the trial.[61] Twenty lawyers were involved in the trial for the Crown, six for Malik and eleven for Bagri. In addition, two lawyers acted as counsel for the court. Reyat hired a team of nine lawyers to work on his defence before finally entering his plea.[62]

Twelve rulings were published on issues of law during the trial. Four rulings resulted from applications by the Crown to vacate a previous editing order,[63] have witnesses declared hostile[64] or have hearsay evidence declared admissible.[65] Three rulings related to applications by Bagri to limit the evidence admissible for the Crown's case[66] and to obtain declarations that Bagri's *Charter* rights had been violated because of destroyed evidence[67] and late disclosure.[68] Another ruling resulted from an application by Malik to have hearsay evidence declared admissible,[69] and two rulings resulted from applications by both accused on issues of disclosure[70] and the admissibility of other hearsay evidence.[71] Other rulings followed an application by the media for access to search warrants and related information[72] and a witness's application, opposed by the media, for a permanent publication ban about the witness's identity.[73]

On March 16, 2005, the accused were both acquitted in a judgment that was 1,345 paragraphs long.[74] Justice Josephson concluded that the involvement of the accused in the offences had not been proved beyond a reasonable doubt and that as a result it was not necessary to address the *Charter* breaches that had occurred because of lost or destroyed evidence[75] and late disclosure.[76]

The proceedings involving Malik and Bagri lasted nearly four-and-a-half years. Fifteen months elapsed between the arrest of the first two accused and the beginning of the pre-trial motions, which were then argued over a period of almost a year. The trial itself began nearly two-and-a-half years after the arrest of Malik and Bagri. The filing of a new indictment adding Reyat caused additional delay, not only because of the presence of another accused who could make pre-trial applications, but also because his counsel required time to become familiar

---

61 As reported in the British Columbia Ministry of Attorney General, Court Services Branch, *Report of the 2002/2003 Fiscal Year* (June 25, 2003), p. 7, online: Legislative Assembly of British Columbia <http://www.llbc.leg.bc.ca/public/PubDocs/bcdocs/348810/csb_annual_report_2002_2003.pdf> (accessed July 7, 2009).

62 *HMTQ v. Malik, Bagri and Reyat*, 2001 BCSC 1758 at para. 4.

63 *HMTQ v. Malik and Bagri*, 2003 BCSC 887.

64 *R. v. Malik and Bagri*, 2003 BCSC 1428, 194 C.C.C. (3d) 572; *R. v. Malik and Bagri*, 2004 BCSC 149.

65 *R. v. Malik and Bagri*, 2004 BCSC 299, 26 B.C.L.R. (4th) 320.

66 *R. v. Malik and Bagri*, 2003 BCSC 1387.

67 *R. v. Malik and Bagri*, 2004 BCSC 554, 119 C.R.R. (2d) 39.

68 *R. v. Malik and Bagri*, 2004 BCSC 1309, 124 C.R.R. (2d) 270.

69 *R. v. Malik and Bagri*, 2004 BCSC 812.

70 *HMTQ v. Malik and Bagri*, 2003 BCSC 1709.

71 *R. v. Malik and Bagri*, 2004 BCSC 819.

72 *HMTQ v. Malik and Bagri*, 2003 BCSC 993.

73 *R. v. Malik and Bagri*, 2004 BCSC 520.

74 *R. v. Malik and Bagri*, 2005 BCSC 350.

75 *R. v. Malik, Bagri and Reyat*, 2002 BCSC 864; *R. v. Malik and Bagri*, 2004 BCSC 554, 119 C.R.R. (2d) 39.

76 *R. v. Malik, Bagri and Reyat*, 2002 BCSC 484; *R. v. Malik and Bagri*, 2004 BCSC 1309, 124 C.R.R. (2d) 270.

with the case. Justice Josephson refused to order a severance for Reyat,[77] and no additional preparation time was given to Reyat's counsel.[78]

9.2.1 Project Management

Well before charges were laid in the Air India trial, the BC Ministry of Attorney General recognized the need for a project management approach to the case to ensure that legal and administrative functions were fully integrated. A project management team was created and a project manager appointed.

The project management team was to deal with all the administrative and inter-ministerial matters to ensure that the prosecutors were not distracted from the legal aspects of the case. The team was also the main point of liaison in the BC Ministry of Attorney General for federal and foreign agencies, and for negotiating and applying the policies, protocols and guidelines that defined the tasks of each agency and settled issues of personnel, budgets, facilities and technology.[79]

Early on, the project management team, including members of the prosecution team, contacted the team working on the trial of those accused of bombing the Pan Am flight that crashed at Lockerbie, Scotland in 1988. It was felt that the Air India project management team could benefit from the wealth of knowledge and experience gained by those managing the Lockerbie trial. It was the project manager's responsibility to oversee the Air India team's relations with the Lockerbie team.[80] The project management and prosecution teams had numerous meetings with their Lockerbie counterparts.[81] Wright and Code wrote that these visits proved "invaluable" for the Air India prosecution.[82]

From the very early stages of the case, the project management team received support from the BC Government. According to Robert Wright, the senior Crown prosecutor, and Michael Code, acting for the defence, this ensured that "…the project management approach and support for the team were coordinated across the justice organization and fully understood and supported by decision-makers (Court Services for the courtroom, Management Services for finance and personnel, Justice Services for defence funding issues, Corrections)."[83] The project manager also recommended creating a steering committee and working group structure that "crossed normal branch barriers."[84]

---

77 *HMTQ v. Malik, Bagri and Reyat*, 2001 BCSC 1758.
78 *HMTQ v. Malik, Bagri and Reyat*, 2001 BCSC 1758.
79 Wright and Code Report on Air India Trial, Part I, pp. 2, 4. Foreign agencies included the FBI (U.S.) and the Irish Gardia.
80 Wright and Code Report on Air India Trial, Part I, p. 23.
81 Wright and Code Report on Air India Trial, Part I, pp. 1-2. The visits to Scotland and The Netherlands also enabled the Crown to meet with members of court services, sheriff and police agencies involved in the Lockerbie trial and to tour the Lockerbie courtroom complex in Kamp van Zeist in the Netherlands, with its state-of-the-art technology, live-note reporting, security arrangements, victims' safe haven and complex translation system.
82 Wright and Code Report on Air India Trial, Part I, p. 2.
83 Wright and Code Report on Air India Trial, Part I, p. 2.
84 Wright and Code Report on Air India Trial, Part I, p. 3. One example of this was the cross-agency committee that was created for building Courtroom 20 specifically for the Air India trial.

One of the main responsibilities of the project manager was to be lead negotiator with the federal government for the funding agreements in the case.[85] At all times, the project manager had to maintain strong links with the head of the prosecution service and the justice ministry to ensure ongoing ministerial support for the trial.[86]

Wright and Code reported that "…the project manager role [evolved] into a general manager role once the main planning stage was finished and the plan implemented."[87] However, the project manager remained responsible for coordinating the efforts of the services and agencies that participated either indirectly or directly in the Air India trial.[88]

9.2.2 The Disclosure Process

Wright and Code described the volume of documents involved in the Air India trial as "vast." The initial trial material provided by the RCMP to the Crown in 1999 was 500,000 pages long. The narrative was contained in 90 volumes. Additional materials followed, including 40,000 lbs. of reel-to-reel tapes from CSIS.[89] Geoffrey Gaul was the media spokesperson during the Air India trial and in 2003 became Director of the Criminal Justice Branch in the BC Ministry of the Attorney General. He testified before the Commission that at one point the Crown had tens of thousands of additional documents arriving.[90]

Gaul testified that the Air India prosecution team saw the importance of preparing, before charges were laid, the materials that would have to be disclosed to the defence:

> [O]ur task at the front-end, we recognized that there was no point in engaging in a charge assessment, a pre-charge, until the file was formatted in a way that should we reach the point of approving a charge, we would then be in a position to provide prompt disclosure….
>
> Lay a charge and then go "Holy cow, we have to organize this to fairly disclose it to the defence", that can take months if not years. You can imagine the delay problems, Mr. Commissioner. We have an accused who's now been charged. The format of disclosure is unfriendly and the Crown is scrambling to unscramble the egg and put it in a format that we can disclose it.

---

85 Wright and Code Report on Air India Trial, Part I, p. 3.
86 Wright and Code Report on Air India Trial, Part I, p. 4.
87 Wright and Code Report on Air India Trial, Part I, p. 3.
88 Wright and Code Report on Air India Trial, Part I, p. 4.
89 Wright and Code Report on Air India Trial, Part II, p. 11.
90 Testimony of Geoffrey Gaul, vol. 88, December 4, 2007, p. 11357.

> So what we did in this case, we did a lot of front-end, an enormous amount of front-end work, of getting the file ready so that when we did our charge assessment, we approved a charge, we were able to disclose it.[91]

In a 2001 decision relating to Malik and Bagri, BC Associate Chief Justice Dohm described the enormity of the expected defence tasks in reviewing disclosure. These included the following:

- complete review of 93 binders of recently disclosed materials;
- review of a "second tier" of Crown disclosure, which was to include 170,000 documents containing 600,000 to 1,000,000 pages and a 33-volume index;
- review of all CSIS and RCMP wire materials, which appeared to contain hundreds of hours of conversations. ACJ Dohm reported the understanding of the defence that there were *Criminal Code* wiretaps which ran for seven to eight months, and years of CSIS wiretaps; and
- review of any further materials which were to be disclosed by the Crown, including those provided to the defence by way of disclosure applications.[92]

Justice Josephson found that CSIS was obliged to comply with *Stinchcombe*[93] disclosure requirements.[94] This gave rise to the possibility of litigation about disclosure of information pertaining to national security.

There were "tiers" of disclosure in the Air India trial. The first involved providing both hard copy and electronic copies of the material. The second involved electronic disclosure only. The third involved making a large volume of files available to the defence for manual inspection.

Gaul testified that the Air India prosecution team decided to use electronic disclosure. The trial brief or the "Crown brief" – the summary of the materials that the prosecution would use as the core of its case – was disclosed both electronically and in about 90 volumes of hard copy.[95] Gaul described a second tier of electronic disclosure as covering the "…rest of the evidence that might well have been relevant to the defence but was not going to form a portion of the prosecution."[96]

---

91 Testimony of Geoffrey Gaul, vol. 88, December 4, 2007, pp. 11366-11367.
92 *Malik and Bagri v. HMTQ*, 2001 BCSC 2 at para. 16.
93 *R. v. Stinchcombe*, [1991] 3 S.C.R. 326.
94 *R. v. Malik, Bagri and Reyat*, 2002 BCSC 864 at paras. 9-10, 14.
95 Testimony of Geoffrey Gaul, vol. 88, December 4, 2007, pp. 11366-11367.
96 Testimony of Geoffrey Gaul, vol. 88, December 4, 2007, p. 11368.

Wright and Code noted that no private law offices in Vancouver at the time the charges were laid were equipped with the computer equipment or expertise to handle disclosure on the scale of the Air India case, especially in electronic form.[97] To remedy this, the Crown negotiated with each defence team to provide the appropriate computer equipment and applications to handle the disclosure.[98]

Another issue was the equipment to be sent to the accused, since they were in preventive detention awaiting trial. For this, the Project Manager worked with Corrections sheriffs to ensure the security of data throughout the trial.[99]

The Crown proceeded with electronic disclosure, maintaining close contact with the defence teams about information technology issues that might arise.[100] A database for every disclosure transaction was also created to avoid confusion about which information had or had not been disclosed.[101]

Code testified about a third tier of disclosure involving "peripheral material" in the filing rooms – "…rooms and rooms and rooms of documents that nobody had even looked at but that you couldn't say that they were clearly irrelevant; they still met the *Stinchcombe* standard." Because it was inefficient for the Crown to scan and disclose these documents electronically, the Crown and defence established a procedure to give counsel access to the documents in a file room on an undertaking of confidentiality. It was the responsibility of defence counsel to review these documents. If they found documents of interest, they would ask for photocopies and take the photocopies back to their offices.[102]

Undertakings: The Crown and defence agreed on three defence undertakings relating to disclosure. The first undertaking applied where the subject material was voluminous and likely largely irrelevant to the proceedings. In that instance, a copy of the material was physically provided to defence counsel for review at their offices. The undertaking included obligations to keep documents secure and also prohibited defence counsel from disclosing the information further, including to the accused, without Crown consent or a court order. The undertaking required the eventual return of the material to the Crown.[103]

The second undertaking related to material that was to remain in the possession of the Crown, but that would be made available to defence counsel for inspection. This form of undertaking was used for smaller amounts of privileged material that remained at all times in the Crown's possession.[104]

The third undertaking allowed defence counsel to go to the Crown office or CSIS to examine the documents that CSIS had not disclosed or that it

97 Wright and Code Report on Air India Trial, Part I, p. 13.
98 Wright and Code Report on Air India Trial, Part I, p. 13.
99 Wright and Code Report on Air India Trial, Part I, p. 16.
100 Wright and Code Report on Air India Trial, Part I, pp. 15-16.
101 Wright and Code Report on Air India Trial, Part I, p. 14.
102 Testimony of Michael Code, vol. 88, December 4, 2007, pp. 11372-11373.
103 Wright and Code Report on Air India Trial, Part III.
104 Wright and Code Report on Air India Trial, Part III.

had disclosed before in an edited ("redacted") form. Although the material pertained to matters of national security, these matters were largely irrelevant to the proceedings. Defence counsel were able to view the full documents electronically while the documents remained in the possession of CSIS. Defence counsel were permitted to prepare a list of relevant information to which the defence might seek access, but no other notes could be made of the information. The undertaking prohibited defence counsel who signed it from disclosing the information to any person, including clients, without a court order or Crown consent. Counsel could, however, disclose the information to other defence counsel who had signed the undertaking.[105]

The third undertaking stated that the undertaking did not compromise any privilege claim by the Crown, CSIS or the Attorney General of Canada. In almost every case, defence counsel concluded that the material was not relevant to the proceedings.[106] If the defence approached the Crown about a document that was relevant and useful to the defence, Code testified, the Crown would always relieve the defence of the undertaking not to disclose the information.[107]

This third undertaking avoided the need for litigation under section 38 of the *Canada Evidence Act*. As Code testified, "…we negotiated the solutions to disclosure that you would ultimately normally have to litigate."[108] No applications were made under section 38 as a result, so the defence and prosecution teams were never required to undergo the logistically difficult and lengthy process of bringing section 38 issues before the Federal Court.

9.2.3 Services for Family Members of Flight 182 Victims

Shortly after Reyat's guilty plea, the National Parole Board gave the victims' family members an opportunity to register as victims and to submit victim impact statements.[109] This process allowed registered victims to receive updates about Reyat's sentence and any parole eligibility dates.[110] Reyat served his sentence and was released on bail in July 2008 while awaiting trial on perjury charges relating to his testimony in the Air India trial.[111]

Several steps were taken to ensure that victims' families could attend the trial and witness the judicial process first-hand. In British Columbia, the *Crime Victim Assistance Act*[112] and regulations[113] provide for services and funding

---

105 Wright and Code Report on Air India Trial, Part III.
106 Wright and Code Report on Air India Trial, Part III.
107 Testimony of Michael Code, vol. 88, December 4, 2007, pp. 11375-11376.
108 Testimony of Michael Code, vol. 88, December 4, 2007, p. 11384.
109 Maryam Majedi, *Air India Victim Services Legacy* (April 2005), para. 28 [*Air India Victim Services Legacy*]. Ms. Majedi was Manager of the Air India Prosecution Team's Victim Services, Criminal Justice Branch, BC Ministry of Attorney General.
110 *Air India Victim Services Legacy*, para. 28.
111 "Convicted Air India bombmaker Inderjit Singh Reyat free on bail" (July 10, 2008), online: CBC News <http://www.cbc.ca/canada/british-columbia/story/2008/07/10/bc-reyat-bail-posted.html> (accessed December 2, 2008).
112 S.B.C. 2001, c. 38.
113 B.C. Reg. 161/2002.

for immediate family members of victims of certain criminal offences and give significant discretion to the Director of Crime Victim Assistance[114] to pay the travel and other expenses of immediate family members to attend legal proceedings.[115] Total assistance is limited to $3,000 per family member.[116]

On October 27, 2000, when charges were laid against Malik and Bagri, BC's Crown Victim Witness Services informed the known family members of the Air India victims of the charges and inquired whether they wanted further contact about the proceedings.[117] Shortly after that, a special program (the Program) was established to provide comprehensive assistance to immediate family members both before and during the trial. The BC Ministry of Attorney General created the Air India Crown Victims and Witnesses Service (AICVWS), which became responsible for managing the Program.[118]

One of the first tasks of the AICVWS was to find the family members who had not yet been located. Out the 487 family members listed in the AICVWS database, the Service established contact with 376.[119] The remainder could not be located, had died or requested that they not be contacted further.[120]

Once accredited, up to two family members from each victim's family unit received travel, accommodation, meal allowances and travel insurance to attend the trial for one week.[121] "Family member" was defined as the spouse, parent, child, sibling, grandparent, aunt or uncle of a deceased victim.[122] The AICVWS also accommodated special circumstances at the accreditation stage, allowing more than two family members to travel where one or more of the accredited family members was frail (elderly or sick) and required a companion for support. The AICVWS also made exceptions where the deceased's family had separated into two non-communicating parts.[123]

Family members of victims came from as far away as India, Saudi Arabia, Sri Lanka and Australia. This imposed additional management duties and costs.[124]

Another problem lay in managing the flow of information to victims' family members, since the AICVWS thought, from the outset, that keeping them

---

114 Section 18 of the *Crime Victim Assistance Act* allows the minister to designate a public service employee as Director.
115 B.C. Reg. 161/2002, s. 23(3)(a).
116 B.C. Reg. 161/2002, s. 23(5).
117 See *Air India Victim Services Legacy*, para. 3.
118 The same organization is referred to as "Air India Victim/Witness Services (AIVWS)" in *Air India Victim Services Legacy*.
119 *Air India Victim Services Legacy*, para. 8.
120 *Air India Victim Services Legacy*, para. 8.
121 Air India Victim/Witness Services Department, Ministry of Attorney General (BC), *Victim Services Handbook*, pp. 43, 46 [Air India Victim Services Handbook].
122 Air India Victim Services Handbook, p. 41.
123 Wright and Code Report on Air India Trial, Part I, p. 17.
124 Wright and Code Report on Air India Trial, Part I, p. 18.

informed was an important objective.[125] This was accomplished through means that included a secure website, newsletters, a handbook for victims, funding for travel to attend the trial, visits to the warehouse housing forensic evidence (the partially-reconstructed aircraft), meeting space in Crown offices, victim services staff and counsellors, regular briefings of visiting victims' family members by the head prosecutor, production of a remembrance book, telephone and email contact with their homes, and regional group meetings with Crown, police and victims.[126]

The Program assigned five AICVWS caseworkers and one lawyer to assist the victims' family members during the Air India trial and for some time after.[127] Caseworkers paid special attention to family members during portions of the Crown's evidence that were expected to be more emotionally charged, such as the testimony of the Irish rescue workers who attempted to recover the victims' bodies.[128]

AICVWS caseworkers began preparing for the verdict as early as May 2004. The weekend before the verdict was pronounced, the AICVWS, the Air India project manager, the head prosecutor and the head of the RCMP Air India Task Force met with local and visiting family members to discuss the possible verdict and to answer questions.

A total of 77 family members, friends and witnesses attended the verdict proceedings on March 17, 2005. After the verdict was rendered, the lead prosecutor, the Crown's media liaison and the head of the RCMP Air India Task Force gave a debriefing session. AICVWS caseworkers were on hand with numerous counselling strategies to deal with the emotional outpouring that might follow. These caseworkers helped many family members through this difficult time. Their help was especially important since some family members had not received any counselling in 1985 immediately after the tragedy.

Section 722 of the *Criminal Code* permits family members of deceased victims to submit victim impact statements on sentencing. However, since both Malik and Bagri were acquitted and there was no sentencing, the section 722 provision did not apply.

Although Reyat had been convicted in 2003 of manslaughter, family members were not asked to submit victim impact statements at that time. Nevertheless, in his decision on sentence, Justice Brenner quoted with approval the comments of the lead prosecutor who, when speaking about the impact of the tragedy on the family members, said: "The immensity of this catastrophe is almost indescribable."[129]

---

125 Wright and Code Report on Air India Trial, Part I, p. 18.
126 Wright and Code Report on Air India Trial, Part I, p. 18.
127 See the names and biographies of caseworkers and legal counsel in Air India Victim Services Handbook, pp. 66-70.
128 This testimony is reflected in *R. v. Malik and Bagri*, 2005 BCSC 350 at paras. 40-48.
129 *R. v. Reyat*, 2003 BCSC 254 at para. 12.

9.2.4 Trial Costs

Victim Services: The total cost for the AICVWS and the Program came to $1.8 million. Although the Program was entirely managed by the AICVWS, which was part of the BC Ministry of Attorney General, the federal government assumed the entire cost.[130]

Prosecution Costs: The BC Ministry of Attorney General reported on the expenditures made by BC to mount the trial, excluding police costs. Prosecution costs associated with the trial started with preparations by a small prosecution team in 1996 and ended in March 2005 with the acquittal.[131] The expenditures were broken down into the following categories and amounts:

Pre-trial[132]	$ 5,610,144
Prosecution except for Witnesses and Victim Services	$13,249,967
Expert and non-expert witnesses[133]	$ 1,759,333
Victim Services	$ 1,766,623
Prosecution total[134]	**$22,386,067**

Defence Costs: Shortly after the charges were laid, Bagri was declared eligible for legal aid funding because of the complexity of the case and the significant preparation time that had been given to the Crown. This happened even though Bagri's income and net worth would normally have made him ineligible. Reyat was also found to be eligible for legal aid when his name was added to the indictment, mainly because he was then in custody and had no way to fund his defence.

Malik, however, did not meet the legal aid criteria in BC and was deemed ineligible. At his bail hearing, he estimated his net worth at $11.6 million. Nonetheless, in February 2002, he reached an interim funding agreement with the Attorney General of BC. This ensured that funding could be applied immediately to his defence costs while he liquidated his assets. As of September 19, 2003, the Attorney General of BC had paid more than $3.6 million to Malik's 11-member defence team under the interim funding agreement. At that time, Malik argued that his defence would require about an additional $2.7 million, plus several hundred thousand dollars in computer costs, to complete the trial.[135] Malik also claimed that he had personally paid $650,000 in legal fees to that date.[136]

---

130 Ministry of Attorney General (BC), *Factsheet: Statement of Expenditures for the Air India Trial*, 2005AG0036-001081 (November 23, 2005), p. 1, online: Government of British Columbia <http://www2.news.gov.bc.ca/news_releases_2005-2009/2005AG0036-001081-Attachment1.pdf> (accessed November 28, 2008) [Air India Statement of Expenditures].

131 Air India Statement of Expenditures, p. 1, fn. 1.

132 This figure does not include expenditures relating to the trial and conviction of Reyat in 1991: Air India Statement of Expenditures, pp. 1-2.

133 The Crown called a total of 90 witnesses (including experts and laypersons).

134 Air India Statement of Expenditures, p. 1.

135 A history of this agreement, as well as the amounts advanced to Malik, can be found in *HMTQ v. Malik*, 2003 BCSC 1439, 111 C.R.R. (2d) 40 at paras. 2, 4-15.

136 *HMTQ v. Malik*, 2003 BCSC 1439, 111 C.R.R. (2d) 40 at para. 17.

Malik applied for funding by way of what is known as a "Rowbotham application" after disagreements arose with the Attorney General of BC about his solvency and unsecured debts.[137] A hearing was held in the summer of 2003 and a decision was rendered on September 19, 2003.[138] There, the Attorney General of BC conceded that Malik could not receive a fair trial without the assistance of counsel.[139] Still, the judge found that Malik was not entitled to funding for his defence since he was not indigent and had not made the necessary efforts to obtain funds to cover his defence. The judge found that Malik could pay the balance of his defence costs and take any measures necessary to reduce those costs, but made no finding as to the past funding provided by the state.[140]

Despite this decision, the Attorney General of BC advanced further funds to Malik for the duration of the Air India trial, based on terms of the interim funding agreement, which was amended periodically to take into account the changing nature of Malik's case.

The province took security against property owned by each co-accused and would seek reimbursement under the terms of the agreement.

BC's *Freedom of Information and Protection of Privacy Act*[141] protects personal information about individual agreements. However, the BC Ministry of Attorney General provided some insight into the extent of funding for the three co-accused, estimating their combined funding to total over $21 million. This represented all the defence costs advanced, either through loan or grant, since the laying of the charges in 2000.[142] Another $358,000 was added for administrative costs related to the defence,[143] for a final total of $21.4 million.[144]

Media reports in November 2005 quoted BC Attorney General Wallace Oppal as saying that Bagri still owed the government $9.7 million and that Malik owed $6.4 million.[145]

---

137 *HMTQ v. Malik*, 2003 BCSC 1439, 111 C.R.R. (2d) 40. *R. v. Rowbotham* (1988), 41 C.C.C. (3d) 1 established that anyone charged with a serious criminal offence and who has been denied a referral to a legal aid lawyer can apply to a judge to appoint a lawyer for them.

138 *HMTQ v. Malik*, 2003 BCSC 1439, 111 C.R.R (2d) 40.

139 *HMTQ v. Malik*, 2003 BCSC 1439, 111 C.R.R. (2d) 40 at para. 1.

140 *HMTQ v. Malik*, 2003 BCSC 1439, 111 C.R.R. (2d) 40.

141 R.S.B.C. 1996, c. 165.

142 Air India Statement of Expenditures, p. 1.

143 These administrative costs included printing and photocopying as well as the computer equipment necessary to view and search the electronically-disclosed evidence.

144 Air India Statement of Expenditures, p. 1.

145 As quoted in reports published by the *Vancouver Sun*, *The Province*, *Times Colonist* and *The Globe and Mail* on November 24, 2005.

Summary of Costs

The BC Ministry of Attorney General estimated the total expenditures for the Air India Trial, before the federal contribution, at just under $58 million.

Courts - Trial Support and Security Operating Expenditures	**$7,753,052**
Prosecution Expenditures	
Pre-trial	$5,610,144
Prosecution except for Witnesses and Victim Services	$13,249,967
Expert and non-expert witnesses	$1,759,333
Victim Services	$1,766,623
Prosecution total	**$22,386,067**
Justice Services Expenditures	
Defence Funding	$22,026,914
(Less PST charges included)	($945,105)
Defence Funding before PST	$21,081,809
Administrative	$357,717
Justice Services total	**$21,439,526**
Corrections - Operating/Custody Expenditures	**$1,958,581**
Management Services - Administrative Support Expenditures	**$230,718**
Total Expenditures before Amortization Expense	**$53,767,944**
Amortization Expense	
Capital costs	$7,825,453
Less: net book value	$3,815,903
Air India Share	**$4,009,550**
Total Expenditures before Federal Contributions	**$57,777,494**[146]

9.2.5 Federal-Provincial Cost-sharing

The federal government and the BC Ministry of Attorney General negotiated a cost-sharing agreement for the Air India trial. Shortly after the charges were laid and before entering the agreement, the federal government granted $1 million to the Ministry. In 2001, under the concluded agreement, the federal government agreed to pay roughly half the total costs of the Air India trial, including all costs related to the AICVWS.[147] Excluded from the agreement were the capital costs

146 Not included in this figure are any wind-up costs in 2005/06: Air India Statement of Expenditures, pp.1-2

147 Air India Statement of Expenditures, p. 1.

incurred by BC, mainly for building the high-security Courtroom 20 where the trial took place.[148]

The BC Ministry of Attorney General estimated that the federal government contributed a total of $27.5 million, leaving a total expenditure by the Ministry of $30.3 million.[149]

9.3 Making Terrorism Trials Workable

Several events could have prevented the Air India trial from reaching a verdict. The trial might have proceeded with a jury. Once a trial by 12 jurors starts, the discharge of more than two jurors due to illness or personal hardship results in a mistrial. Even if ten jurors could have lasted for the duration of the trial, more frequent breaks would have been required than in a judge-alone trial to accommodate matters such as the illness of jurors. The trial judge could have become incapacitated; in the case of a judge-alone trial, the entire trial would have had to start anew. Counsel might have ignored their professional duties as officers of the court and employed tactics such as frivolous applications, including those requiring litigation in the Federal Court and interlocutory appeals, calling unnecessary witnesses, engaging in excessive cross-examination, refusing to agree to non-contentious facts and attempting to appeal adverse findings before the trial was completed. Such tactics could have delayed the trial beyond repair. If lead counsel had been inexperienced, they might have lacked the judgment to avoid avenues of prosecution or defence that would have further delayed or complicated the trial.

If less well-organized, the Crown might not have been able to cope with the enormity of the disclosure obligations. This would have led to a stay. If relations among defence and prosecution teams had deteriorated,[150] cooperation would have also diminished, perhaps preventing agreement on the *ad hoc* procedure for dealing with issues that otherwise would have brought litigation under section 38 of the *Canada Evidence Act* into play, which would have greatly prolonged the trial.

In his paper for the Commission, Bruce MacFarlane offered a more generic analysis of the "realities" of terrorism trials, and identified further impediments that could prevent such trials from reaching verdicts:

> Terrorist trials have several important realities. They are usually lengthy and very complex. Crown disclosure obligations often raise difficult national security issues. Those accused of terrorism, at least in Canada, have the right to choose

148 Air India Statement of Expenditures, p. 2.
149 Air India Statement of Expenditures, p. 1.
150 Wright and Code spoke of the "good administrative relationship" between Crown and defence in the Air India trial and how this led to a successful disclosure process and other successfully managed aspects of the trial: Wright and Code Report on Air India Trial, Part I, p. 10.

> trial before a trial and jury, or a judge sitting alone. The acts charged are usually horrific in nature, enraging the public and placing extraordinary pressure on the police and prosecutors to convict those responsible. And politicians sometimes wade into the case, making fair trial requirements even more difficult to meet.
>
> These realities can place a terrorist trial at risk. For a variety of reasons, an unmanageably long trial may never reach verdict: a mistrial may be required where more than two jurors have to be discharged; the trial may abort where the trial judge cannot continue with the case; Crown mismanagement or the simple reality of its disclosure obligations may force a judicial stay; defence demands for disclosure of security-sensitive information may, if successful, force the Crown to terminate the case to protect the information; and, if the case reaches "mega" proportions, the simple passage of time can lead to the evidentiary collapse of the Crown's case, prompting a Crown stay with no determination on the merits of the evidence. Accused persons, as well, face the risk of not being able to have a fair trial where the acts alleged are so horrific that their simple allegation has had a direct impact on the fabric of society – potentially tainting the pool from which jurors are chosen, and altering normal decision-making by police, prosecutors, scientists and, some would argue, the judiciary.[151]

The Air India trial did reach a verdict. Good management and, in some cases, good fortune allowed the trial to avoid many impediments that might otherwise have seriously delayed, or even scuttled, it. Lessons must be learned from this experience. Nevertheless, the management measures and procedures employed at the Air India trial should not automatically be seen as a template for future terrorism cases. Each case will have its own unique features.

The following section discusses several measures to reduce the risk of terrorism trials failing to reach a verdict. These measures include sound administrative management of the trial, appointing the trial judge early in the process, developing an appropriate disclosure process, organizing the early hearing of motions, ensuring appropriate funding of both defence and prosecution counsel, encouraging judges to take firmer control of the trial and counsel to act more responsibly as officers of the court, and increasing the number of jurors to prevent mistrials in long jury trials. In addition, though not directly germane to the trial reaching a verdict, the dictates of decency require that the terrorism trial process fully address the needs of victims and their families.

The importance of amending section 38 of the *Canada Evidence Act* to allow the trial judge to make and revise non-disclosure orders on the basis of national

---

151 MacFarlane Paper on Terrorist Mega-Trials, p. 293.

security confidentiality was discussed fully in Chapter VII. The section 38 issue will be discussed only briefly here, and only as it relates to the pre-trial management responsibilities of the trial judge.

9.3.1 Project Management

Wright and Code suggested that "…a megacase should be seen not only as a prosecution but as a major administrative project," and called for a project management approach to mega-cases, "…including a project manager, project team, project management planning, budgeting, risk assessment, implementation, monitoring and evaluation."[152]

The project management approach adopted in the Air India trial was an essential part of the trial process. In future trials, project managers may be equally important, addressing the multitude of administrative complexities that can delay or even defeat a terrorism prosecution, and allowing counsel to focus on the legal issues.

9.3.2 Cost-sharing

The Air India trial provided a model for federal-provincial cost-sharing arrangements in future major terrorism trials. Adequate funding is necessary for all aspects of a terrorism trial: for project management and the disclosure process, for the hiring of sufficient numbers of competent and experienced prosecutors and defence counsel, and for the provision of services to victims and their families.

The federal government has a clear interest, and a central role, in terrorism prosecutions. One essential federal role in long and complex prosecutions is to provide financial support. British Columbia faced a bill of over $30 million for the Air India trial, even after the federal government had contributed $27.5 million. Smaller provinces may not have the financial capacity to underwrite such lengthy and complex trials; generous federal cost-sharing will be necessary. As will be seen, federal cost-sharing could also encourage experienced defence counsel to become involved in lengthy terrorism prosecutions. Cost-sharing could also fund proper project management so that counsel can focus on legal issues instead of administrative and logistical details.

9.3.3 The Trial Judge

While many procedural changes can be made to enhance the prospect of terrorism trials reaching a verdict, the pivotal point of the entire process is the trial judge. A competent, experienced judge is essential. That means a judge with criminal law experience, an appreciation of the independence of the judiciary, good health and a readiness to take on what may turn out to be a very lengthy case.

---

152 Wright and Code Report on Air India Trial, Part I, p. 2.

Wright and Code identified certain qualities that the judge should possess:

> You need a trial judge who is bright, experienced and fair and who is patient and able to listen for a long time.… Because mega-trials generally cannot be repeated, there is a high premium on choosing a trial judge who will not make reversible errors. This means choosing from the brightest, most experienced and fairest judges. At the same time, the extreme length of these cases means that you must choose a judge who will remain patient and not try to take over the case, as it will inevitably drag on.[153]

In a recent article Code argued that the judiciary is afraid to control counsel. He called for a clear legislative statement to declare the existing common law powers of the judiciary:

> It needs to be clarified that the courts have the power to enforce these particular duties, and thus to require that counsel "act responsibly", in order to ensure a fair and efficient trial. The judiciary fear intervening in this area due to concerns about perceived partiality, and the law societies almost never use their discipline processes to enforce these basic tenets of professionalism, all of which are set out in the Rules of Professional Conduct. As a result, counsel's ethical duties as officers of the court are rarely enforced. A clear legislative statement on the point would resolve any uncertainty about judicial powers to enjoin and sanction counsel in this sphere and would encourage enforcement of the basic requirements of professionalism. Such a statement would only need to be declaratory of the existing common law as this kind of modest approach has often been helpful in educating the bench and bar and encouraging cultural change within the justice system.[154]

At trial, the trial judge must not be timid in controlling the conduct of counsel and should not hesitate to rein in counsel who, for example, bring dilatory motions, present massive and unnecessary amounts of irrelevant evidence or conduct excessive cross-examinations. However, the authority to control the excesses of the adversarial process is not a licence for the judge to descend into the forum. The latter is not permitted, whereas the former is a necessary part of the judge's obligations to ensure a fair trial.

The trial judge should be appointed early to allow the judge to become involved from the start in managing the trial. In the terrorism context, a trial judge who

---

153 Wright and Code Report on Air India Trial, Part II, p. 1.
154 Code Article on Mega Trial Phenomenon at 467.

is appointed early can take control of the pre-trial process and establish rules to avoid the process being derailed. Early nomination of the trial judge also gives the judge greater "ownership" of the case. It allows the judge to establish procedures, and, in particular, allows the judge to make it clear to counsel the level of professionalism that is expected of them.

Appointing trial judges early also allows them to deal with disclosure, since disclosure issues are most often dealt with in the early stages of the trial process. At the same time, early appointment of trial judges ensures that they will not face the burden of handling files from other cases as they are trying to get the terrorism trial process underway. Although it may cause scheduling difficulties in some jurisdictions, early appointment is necessary. At present, only trial judges have the legal power to make binding rulings on matters such as the admissibility of evidence and *Charter* motions.[155] Early appointment of a trial judge would also be facilitated if, as recommended in Chapter VII, a chief justice selects a trial judge who can decide national security confidentiality matters under section 38 of the *Canada Evidence Act* as well as other disclosure issues and pre-trial motions. Such a comprehensive approach to pre-trial management would follow international best practices as seen in Australia, the United Kingdom and the United States.[156]

9.3.4 Defence and Crown Counsel

9.3.4.1 Funding

At its peak, the Air India trial involved 46 Crown and defence lawyers, with the three defence teams totalling 26 lawyers.

Wright and Code argued that the prosecution in such cases should be headed by a "…senior crown counsel with leadership credentials, experienced in both complex, difficult trials and administrative matters," since both skill sets are bound to be critical in weathering the many challenges that can arise throughout the pre-trial and trial phases of any mega-trial.[157] Wright and Code suggested that the lead prosecutor must have a "…resilient, pragmatic and flexible personality" to "…negotiate the innumerable procedural and substantive issues with the defence, so that the trial proceeds in a reasonably efficient manner."[158] They added:

> In particular, disclosure, admissions, procedural and evidentiary motions and scheduling will be the subject of continuous discussions over a number of years, as the case proceeds. The Crown inevitably must take the lead in these

155 *R. v. Rahey*, [1987] 1 S.C.R. 588*; R. v. Litchfield*, [1993] 4 S.C.R. 333; *R. v. Hynes*, 2001 SCR 82, [2001] 3 S.C.R. 623.
156 Roach Paper on Terrorism Prosecutions, pp. 248-287.
157 Wright and Code Report on Air India Trial, Part I, p. 5.
158 Wright and Code Report on Air India Trial, Part II, p. 2.

> discussions, as the Crown has the burden of moving the case forward. For these discussions to succeed the lead prosecutor must be a skilled and pragmatic negotiator who does not insist on winning every small point and who is not deterred by any of defence counsel's failings. . . . If every little point has to be fought, the "mega-trial" will never end.[159]

For similar reasons, Wright and Code recommended that the accused's defence should be conducted by experienced and senior counsel who have good judgment and who understand "…the delicate balance between counsel's duty to their client and their duty to the court." This includes "…a strong element of public interest . . . which obliges counsel to pursue justice in an efficient and expeditious manner."[160] Such senior defence counsel would know "…which issues are worth pursuing, which issues should be discarded and which issues can be satisfactorily resolved through negotiations with the Crown."[161]

Canada's largest and most complex trials should be handled by the most capable and experienced lawyers, but the ability of some governments and virtually all accused to pay for these lawyers remains a significant problem. The Air India trial showed the extensive prosecution and defence costs that may be involved in future terrorism trials. As described earlier in this chapter, prosecution costs totalled over $22 million[162] and the estimated defence costs for Reyat, Malik and Bagri totalled over $21 million.[163]

Wright and Code emphasize the importance of providing adequate funding for the defence:

> From the defence perspective, experienced and senior counsel will simply not take on such a case without appropriate resources as it requires counsel to essentially give up the rest of their practice. Furthermore, every step taken by a well-resourced Crown and police team has to be matched or responded to by the defence. Significant resources are required before the trial even starts simply to read the voluminous disclosure, to retain private investigators, to interview witnesses and to confer with experts. If the resourcing levels for the Crown and the defence do not reflect some general proportionality, the trial will not be fair and senior and experienced counsel will not participate. On the other hand, if the resourcing is too generous it will exacerbate

159 Wright and Code Report on Air India Trial, Part II, p. 2.
160 Wright and Code Report on Air India Trial, Part II, p. 3.
161 Wright and Code Report on Air India Trial, Part II, p. 3.
162 As reported in Air India Statement of Expenditures, p. 1.
163 To this figure must be added more than $350,000 in administrative costs related to the defence: Air India Statement of Expenditures, p. 1.

> the worst features of the "mega-trial"....[D]efence counsel who are guaranteed generous levels of "cash for life" from the public purse will not be eager to return to the challenges of their ordinary practice where retainers are almost always limited. In conclusion, a delicate balance is required between too [few] resources for the Crown and defence and too [many] resources.[164]

They stress the need to avoid the extremes of a "blank cheque" approach to funding the defence or an approach that will make it impossible for experienced counsel with significant overhead expenses and other clients to take on a major case. Providing adequate resources to retain experienced counsel will pay important dividends. It should result in responsible admissions of fact, more focused pre-trial and trial proceedings and less needless conflict between Crown and defence. Otherwise, excessive pre-trial motions and trials and unwarranted conflicts between counsel can greatly prolong a trial and, in extreme cases, prevent it from reaching a verdict.

Legal aid is generally seen as falling within provincial jurisdiction over the administration of justice.[165] However, the federal government has since 1972 treated legal aid as falling within its "overall reform strategy" aimed at addressing poverty, crime and disorder.[166] Since that time, the federal government has agreed to share the cost of criminal legal aid with the provinces. The administration of the legal aid programs remains a provincial responsibility.[167]

A review of provincial eligibility guidelines shows that most accused with full-time employment when arrested are not likely eligible for assistance under their local legal aid schemes.[168] The likely length and complexity of terrorism proceedings will mean that nearly all accused would be unable to afford their legal fees on their own. Even if they were eligible for legal aid, the amount of legal aid funding available would almost certainly fall far short of that needed to retain experienced counsel.

Proper funding is vital for the efficient management of the trial. The cost of experienced counsel may seem high, even extraordinary, to an outside observer,

---

164 Wright and Code Report on Air India Trial, Part II, p. 3.

165 *Constitution Act, 1867* (U.K.), 30 & 31 Vict., c. 3, reprinted in R.S.C. 1985, App. II, No. 5, s. 91(24).

166 Karen Hindle and Philip Rosen, "Legal Aid in Canada" (Parliamentary Information and Research Service, Library of Parliament, August 6, 2004), p. 4, online: Government of Canada <http://dsp-psd.pwgsc.gc.ca/Collection-R/LoPBdP/PRB-e/PRB0438-e.pdf> (accessed December 3, 2008) [Legal Aid in Canada].

167 The Federal-Provincial Agreement on Legal Aid in Criminal Matters, signed in December 1972, established a cost-sharing arrangement between the federal government and the provinces: Legal Aid in Canada, p. 4.

168 However, some legal aid laws allow the government to take into account special circumstances and grant legal aid in cases where it would normally be denied. See, for example, Quebec's *Legal Aid Act*, R.S.Q. c. A-14. Section 4.3 provides that, where exceptional circumstances warrant and in order to avoid the occurrence of irreparable harm, the administrative committee may rule that a person who is ineligible for legal aid is in fact eligible on payment of a contribution (as interpreted in *Attorney General of Quebec v. R.C.* (also cited as *Quebec (Attorney General) v. R.C.)*, [2003] R.J.Q. 2027 (C.A.) at para. 13.

but the increase in the efficiency of the trial process is more than likely to offset the increased cost. The undertakings reached in the Air India trial between defence and prosecution about disclosure, particularly disclosure that might otherwise have required national security confidentiality litigation under section 38 of the *Canada Evidence Act*, for example, were the mark of experienced counsel. Those undertakings prevented debilitating delays and possibly even the collapse of the case, both of which would have imposed significant further costs.

In *R. v. Rowbotham*,[169] the Ontario Court of Appeal held that the denial of state-funded counsel to an indigent, unrepresented accused facing serious and complex criminal charges violated the rights to a fair trial and to make full answer and defence under sections 7 and 11(d) of the *Charter*. The appropriate remedy in these circumstances was a conditional stay of proceedings pending the appointment of state-funded counsel by the appropriate Attorney General or legal aid program. The prosecution could not proceed unless the Government agreed to pay for the accused's lawyer.[170]

For cases that present additional special circumstances, an accused may file a "Fisher application" for a court order that the Government fund the case at levels exceeding ordinary legal aid rates. Named after the leading case, *R v. Fisher*,[171] a Fisher application is in essence a special type of Rowbotham application. A Fisher application typically involves a request for funding to pay for higher fees, extra preparation time, additional defence lawyers and other forms of enhanced services.[172] In several provinces, Fisher applications have succeeded where the trial is exceptionally long and complex. Nonetheless, debate continues about whether the courts have the authority to order governments to provide this increased funding.[173]

Rowbotham and Fisher applications will increasingly be a feature of terrorism trials, given the likely size of the files, the complexity of the evidence and the need to involve experienced lawyers to ensure that the trials proceed efficiently and fairly. If at all possible, decisions about funding defence counsel should be made without such applications. The courts will impose a solution if they must,[174] but it would be better for all concerned if governments could reach prompt agreements with counsel about funding that will avoid the time and expense of litigating the issue.

Low legal aid tariffs make it very difficult for experienced lawyers to take on long cases. It is one matter to take a short trial at a rate that does not pay the

---

169 (1988), 41 C.C.C. 1.

170 As described in the BC "Legal Services Society Factsheet" [BC Legal Services Society Factsheet].

171 *R. v. Fisher*, 2001 SKCA 136, 217 Sask. R. 134 (Q.B.).

172 *Attorney General of Quebec v. R.C.* (also cited as *Quebec (Attorney General) v. R.C.)*, [2003] R.J.Q. 2027 (C.A.) at para. 168.

173 BC Legal Services Society Factsheet.

174 However, uncertainty remains about whether courts should make orders departing from inadequate legal aid tariffs or if they should stay proceedings: See *Attorney General of Quebec v. R.C.* (also cited as *Quebec (Attorney General) v. R.C.)*, [2003] R.J.Q. 2027 (C.A.) at paras. 6, 163-164, which held that a stay of proceedings was the appropriate remedy but which also recognized that in a long prosecution the Government had agreed to pay counsel fees beyond the regular legal aid rate.

overhead of a successful law practice, but it is quite another to sign up for a year-long trial at such rates. The Lesage and Code recently commented that this can lead to "…a vicious circle: the longer criminal trials become, the less likely it is that leading counsel will agree to conduct them on a Legal Aid certificate; and yet having leading counsel conduct the defence in these cases is one of the solutions to the overly long trial, as it is these counsel who are most likely to conduct the trial in an efficient and focused manner."[175]

British Columbia has taken steps to attract experienced and leading counsel to complex cases by providing an enhanced fee structure and a separate and confidential fee structure for exceptional matters.[176] Federal cost-sharing is one factor that allows British Columbia to do this. Indeed, federal funding facilitated negotiating a consent Fisher order in the Air India trial, and this approach should be used in future terrorism prosecutions. Attempting to save money by insisting on regular legal aid rates for long terrorism prosecutions is short-sighted. It will only add to the length and cost of the trial and may even diminish the chances that the trial will reach a verdict.

9.3.4.2 Conduct of Counsel

Establishing a good working relationship between Crown and defence counsel is an essential precondition to the successful management of any terrorism prosecution. Given the difficult situations that counsel involved in terrorism trials are likely to encounter, it is vitally important that counsel respect and adhere to the rules of professional conduct and demonstrate civility in their relations with each other.

In the Air India Trial, 37 counsel interacted over a 19-month trial, as well as during the pre-trial process, which lasted almost three years and which also involved the nine lawyers representing Reyat. The lawyers had to fulfill their roles in the adversarial system while maintaining sufficient professional courtesy and respect to work together and make appropriate concessions and admissions. Wright and Code spoke of how well this relationship worked:

> The exceptionally good administrative partnerships between Crown and the defence resulted in immense savings in time and money. At the end of final submissions, the trial judge stated that had it not been for this Crown and defence partnership, along with the very effective technology innovations by Court Services and other agency staff, the trial would have lasted at least twice as long.[177]

Lesage and Code noted how admissions made by defence counsel in the Air India trial reduced a list of 883 potential Crown witnesses, with an estimated

175 Lesage and Code Report on Large and Complex Criminal Case Procedures, p. 96.
176 Lesage and Code Report on Large and Complex Criminal Case Procedures, p. 103.
177 Wright and Code Report on Air India Trial, Part I, p. 3.

trial length of three to four years, to 85 Crown witnesses.[178] This underlines how responsible defence counsel who are willing to make reasonable admissions of fact can shorten a complex terrorism trial. Conversely, irresponsible counsel can prolong a trial to the point of making it almost impossible to reach a verdict.

Even during the Air India trial, however, defence lawyers at times expressed concern about their relationships with the prosecution team[179] and even accused some counsel of misleading and sharp practice.[180] Justice Josephson suggested the need for increased courtesy in communications between Crown and defence.[181] He stated that proceedings such as the Air India trial could be made significantly more difficult if a "…reasonable degree of mutual respect and trust between counsel" was not present.[182]

In a recent article, Code stated that there is "…a well documented argument that standards of civility have been in serious decline throughout all segments of society in recent years" and that "…the legal profession has been subject to a number of specific influences, pressures and changes that have made the modern practice of law particularly susceptible to incivility."[183] This decline, he said, is likely to cause more incidents that will require the intervention of trial judges.

LeSage and Code addressed the ethical and legal duties of Crown and defence counsel, as officers of the court, to make admissions of fact. They observed that "…[c]ounsel for the Crown and the defence are both under ethical duties to make reasonable admissions of facts that are not legitimately in dispute. The court should encourage and mediate efforts to frame reasonable admissions. When the defence fully admits facts alleged by the Crown, the court has the power to require the Crown to accept a properly framed admission and to exclude evidence on that issue."[184]

Clearly, the conduct of counsel can have a profound effect on the pre-trial and trial processes, and counsel must remember their ethical obligations. Code identified several ethical duties that apply to counsel as officers of the court which can facilitate trials in mega-cases. These duties would apply equally to counsel in terrorism trials:

> It is obvious that long and complex trials place a particularly high premium on counsel's ethical duties as officers of the court. These duties apply to both the Crown and the defence. Making responsible admissions of matters that

178 Lesage and Code Report on Large and Complex Criminal Case Procedures, p. 103, fn. 133.
179 *R. v. Malik, Bagri and Reyat*, 2002 BCSC 484 at para. 24.
180 2002 BCSC 484 at para. 42.
181 2002 BCSC 484 at para. 40.
182 2002 BCSC 484 at para. 40.
183 Michael Code, "Counsel's Duty of Civility: An Essential Component of Fair Trials and an Effective Justice System" (2007) 11 Can. Crim. L. Rev. 97 at 98 [Code Article on Counsel's Duty of Civility].
184 LeSage and Code Report on Large and Complex Criminal Case Procedures, p. 89.

> cannot realistically be disputed, refusing to make frivolous arguments that have no real basis in fact or law and treating your opponent with respect and courtesy are all hallmarks of the professionally responsible lawyer. When counsel abide by these ethical duties in large complex cases, their conduct will invariably shorten and simplify the trial and the pre-trial motions. The result will be a better quality of justice both for the client and for the overall administration of justice.[185]

It cannot be stressed too much that the trial judge plays a key role in determining the level of civility in the courtroom. It is the judge's responsibility not to remain passive, but to set the tone and to discipline errant counsel. Ultimately, the trial judge is the person in charge and, regrettably, as discussed below, it is not uncommon for trial judges to lose control of the proceedings.

9.3.5 Accountability of the Legal Profession for Trial Delays

Legitimate criticism has been directed at the legal profession for its role in extending the length of trials. This criticism applies to civil and criminal proceedings, but the following discussion addresses criminal proceedings, where lawyers and judges both bear responsibility for the problem.

9.3.5.1 Lawyers

It is essential that constitutional rights granted to Canadians not be placed in jeopardy. However, obstructionist tactics employed under the guise of protecting *Charter* rights are a reality in our justice system. Such tactics are an abuse of the system and a threat to the efficient administration of justice. Regrettably, obstructionist tactics are a frequent occurrence in Canadian courts. When they are allowed to be used, it can fairly be said that the judge has lost control of the court proceedings to some extent.

Evidence of this loss of control is seen in the tolerance of judges for delay tactics and frivolous applications by defence counsel. Though the right to fair answer and defence is unassailable, applications without merit by defence counsel should not be tolerated in light of their duties as officers of the court.[186] Besides being admonished by the trial judge, miscreant lawyers should be reported to the appropriate law society.

Lesage and Code, as well as some judges, have raised concerns about the ability of law societies to discipline lawyers for making frivolous motions that threaten the possibility of deciding a case on its merits.[187] Law societies must

---

185 Code Article on Mega Trial Phenomenon at 463.

186 See, for example, Chapter 10 of Alberta's *Code of Professional Conduct,* addressing the lawyer's role as advocate. Rules 1 and 2 provide, respectively, that "A lawyer must not take any step in the representation of a client that is clearly without merit" and that "A lawyer must use reasonable efforts to expedite the litigation process".

187 Lesage and Code Report on Large and Complex Criminal Case Procedures, p. 141; *R. v. Dunbar* (2003), 191 B.C.A.C. 223 (B.C.C.A); *R. v. Francis* (2006), 207 C.C.C. (3d) 536 at 542-543 (Ont. C.A.).

take their disciplinary mandates seriously when confronted with misconduct in the court room. They should consider robust sanctions, including suspensions from practice and even disbarment, for lawyers who bring genuinely frivolous motions that threaten the viability of long trials. As discussed earlier, adequate funding should also be available to ensure that experienced defence lawyers can afford to take on long terrorism prosecutions. Invoking disciplinary measures and involving experienced counsel in terrorism trials will minimize the chances that terrorism prosecutions will be impaired by needless motions and delaying tactics.

Equally, the conduct of Crown counsel is not beyond reproach. Agents of the Attorneys General are under the disciplinary control of the law society to which they belong.[188] In addition, their conduct of trials is the responsibility of the Attorney General of the province where the trial occurs. Those in charge of Crown counsel should not wait for judges or law societies to take remedial action if unreasonable actions by Crown counsel contribute to prolonged trials. It is important that experienced and reasonable prosecutors be assigned to terrorism prosecutions and that there be effective oversight of their actions.

While delay and ill-conceived applications are, as a rule, the province of defence counsel, the Crown contributes equally to the length of trials by overcharging. In many cases, instead of carefully considering a charge or charges, the Crown lumps several accused together and lays multiple charges of conspiracy and specific offences. This is a particular likelihood under the *Anti-terrorism Act*, which contains many overlapping offences. Overcharging results in long preliminary hearings and lengthy instructions to juries at trial. The corollary of overcharging is that it gives defence counsel the chance to attack legitimately the multiplicity of inappropriate charges. All this serves only to lengthen a trial.

Canadian law societies have a duty to respond when irresponsible actions by their members add to the length of trials. Law societies must respond to complaints, particularly from judges, but they must do more. In today's climate of frequent abuse, it is not sufficient that law societies react only to complaints by the courts or others. Law societies must be more proactive, in order to ensure that all counsel are aware of their ethical duties to the court, including the prohibition against frivolous motions or refusals to make obvious admissions of fact. As Lesage and Code argued, trial judges should also "…insist on high levels of professionalism from all counsel in long complex trials. This should begin with educative steps, to remind counsel of the basic rules of court room behaviour and of their duties as officers of the court. At the first sign of misconduct, the judge should intervene and remind counsel of their proper role."[189]

9.3.5.2 Judges

The increased length of Canadian criminal trials is a recent development. Chief Justice McLachlin recently observed that murder trials which used to take five

---

188 *Krieger v. Law Society of Alberta*, 2002 SCC 65, [2002] 3 S.C.R. 372.
189 Lesage and Code Report on Large and Complex Criminal Case Procedures, p. 179.

to seven days now routinely take five to seven months, if not longer.[190] Other judges have observed how the *Charter* and pre-trial motions have contributed to prolonging trials.[191] However, the judicial contribution to overly long trials has sometimes been overlooked. Judges bear a good part of the responsibility for delay caused by misconduct by counsel, and by endless, pointless applications in their courtrooms. It is important to understand why some judges today are losing control of long trials.

In recent years, there has been a large increase in the number of judges, both provincial and federal. Each judge brings different experiences, strengths and weaknesses to the court room. All judges, however, must be able to conduct themselves in a fully independent manner.

Judicial independence has been a pillar of our judicial system. It may be that not all judges realize the full reach of that independence. Judicial independence can be abused, but history has shown that the benefits of such independence outweigh the risk of abuse. Judicial independence is one of the principle features of a democracy and is essential to the impartial administration of justice. It ensures that a judge cannot be removed simply because the government of the day happens to dislike his or her decisions. Judicial independence is said to put the judiciary in a position where there is nothing to lose by doing what is right and little to gain by doing what is wrong in the performance of its duties.[192]

The independence of the superior courts is entrenched in section 99 of the *Constitution Act, 1867*, which provides that superior court judges hold office during good behaviour and may only be removed by the Governor General on Address of the Senate and House of Commons. The cumulative effect of sections 96 to 100 of the Constitution is to assign the appointment, tenure and removal of superior court judges to Parliament. Judicial independence is also protected under section 11(d) of the *Charter*, which gives a person who is accused of an offence the right to be tried before an independent and impartial tribunal.[193] Finally, judicial independence has been recognized as a fundamental principle of the Constitution that is not limited to the textual provisions described above.[194] Concerns about judicial independence should not be limited to the mechanics of security of tenure, financial security and institutional independence from the legislature and the executive. Concern should also extend to the spirit of judicial independence.

---

190 Rt. Hon. Beverley McLachlin, "The Challenges We Face", Remarks Presented at the Empire Cub of Canada (March 8, 2007), online: Supreme Court of Canada <http://www.scc-csc.gc.ca/court-cour/ju/spe-dis/bm07-03-08-eng.asp> (accessed December 3, 2008).

191 Hon. Michael Moldaver, "Long Criminal Trials: Masters of a System They Are Meant to Serve" (2006) 32 C. R. (6th) 316 at 319[Moldaver Article on Long Criminal Trials]. The remarks were made during the John Sopinka Lecture on Advocacy at the Criminal Lawyers' Association Annual Fall Conference held in Toronto on October 21, 2005.

192 W.R. Lederman, "The Independence of the Judiciary" 1956 (Volume 34) The Canadian Bar Review 1139 at 1179, citing R. MacGregor Dawson, *The Government of Canada*, 2nd ed. (Toronto: University of Toronto Press, 1954), p. 475.

193 *Valente v. The Queen*, [1985] 2 S.C.R. 673; *R. v. Generoux* [1992] 1 S.C.R. 259.

194 *Reference re Remuneration of Judges of the Provincial Court (P.E.I.)*, [1997] 3 S.C.R. 3.

Although the formal requirements of judicial independence continue to be honoured, some judges in some long cases may believe that they are not fully independent. Such perceptions may be inhibiting the ability of trial judges to control a trial. In their recent report, Lesage and Code spoke of how "timid judging"[195] erects a barrier to effective judicial case management, including the trial judge's common law powers to determine schedules, set time limits and impose other requirements with respect to pre-trial motions. The reasons for this timidity must be addressed and, to the extent possible, it must be eliminated.

For a variety of reasons, judges may perceive that they are not fully free to make rulings without fear of consequences. They may fear that exerting tight control over the trial process may lead to claims of reasonable apprehension of bias, reversal on appeal and complaints to their chief justice or to the Canadian Judicial Council. This fear may inhibit judges from exercising the type of judicial independence and power necessary to manage long terrorism trials. The only factor that should influence a stern direction, an unpopular decision or a difficult choice should be the judge's carefully considered opinion.

Fortunately, appellate courts are increasingly recognizing that trial judges must be able to exercise strong case management authority in order to control the trial process. In one recent case involving protracted proceedings, the Ontario Court of Appeal upheld the trial judge's refusal to allow the Crown to lead documentary material on the 67th day of a trial. Justice Rosenberg recognized that "…a trial judge does have and must have a power to manage the trial." He added that, "in exceptional circumstances," case management "…can even include a power to require the prosecution to call its evidence in a particular order."[196] He added:

> The trial judge had spent 67 days of trial with the case. He was intimately familiar with the issues and the potential pitfalls of proceeding in the way suggested by the prosecution. Far from showing impatience or partiality to one side or the other this trial judge had shown considerable patience and restraint. But, he was of the view that something had to be done to bring the case back under control. This was not a demonstration of partiality but an exercise of a trial management power.
>
> Whatever may have been the case in the past, it is no longer possible to view the trial judge as little more than a referee who must sit passively while counsel call the case in any fashion they please. Until relatively recently a long trial lasted for one week, possibly two. Now, it is not unusual for trials to last for many months, if not years. Early in the trial or in the course of a trial, counsel may make decisions that unduly lengthen the trial or lead to a proceeding that is almost

195 Lesage and Code Report on Large and Complex Criminal Case Procedures, p. 16.
196 *R v. Felderhof* (2003), 180 C.C.C. (3d) 498 at paras. 36, 39 (Ont. C.A.).

> unmanageable. It would undermine the administration of justice if a trial judge had no power to intervene at an appropriate time and, like this trial judge, after hearing submissions, make directions necessary to ensure that the trial proceeds in an orderly manner. I do not see this power as a limited one resting solely on the court's power to intervene to prevent an abuse of its process. Rather, the power is founded on the court's inherent jurisdiction to control its own process.[197]

Another case involved devoting five weeks to an issue raised under section 37 of the *Canada Evidence Act*. This involved access to information about an informer. At an appeal taken before trial, Justice Sharpe warned that "…[t]he trial judge certainly could and should have taken a firmer hand in moving this issue along. She entertained lengthy and repetitive submissions that became an ongoing dialogue instead of insisting on focused submissions."[198] The test for reasonable apprehension of bias in a judge is strict. It requires a real likelihood or probability of bias in the eyes of a reasonable and informed person.[199] Trial judges should not allow the remote possibility of reversal on appeal to fetter their exercise of strong case management authority. To this end, it will be helpful if terrorism prosecutions were conducted by trial judges who are experienced and knowledgeable about the complex evidentiary and criminal law issues involved.

Another possible perceived threat to judicial independence is the ability of the Canadian Judicial Council (CJC), which is composed of about 40 chief justices and associate chief justices, to investigate complaints about the judicial conduct of the more than 1,000 federally-appointed judges.

The CJC was created pursuant to section 59 of the *Judges Act*. [200] Under the Act, the CJC has the power to investigate complaints made by members of the public about the conduct of superior court judges. Complaints can be made by anyone, including an unhappy litigant or lawyer who has appeared before the judge.

The Judicial Conduct Committee of the CJC can generally dismiss without further process any complaints that are trivial, vexatious, made for an improper purpose or manifestly without substance, or it can deal with complaints in a summary manner. If the complaint is not dismissed summarily, additional information may be sought from the judge, the judge's chief justice and the complainant, and remedial measures may be imposed. At higher levels, the complaint may be considered by a panel of three or five judges, but the panel may not include a judge from the same court as the judge who is the subject of the complaint. This panel may recommend a formal inquiry, and the CJC may

---

197 *R. v. Felderhof* (2003), 180 C.C.C. (3d) 498 at paras. 39 and 40 (Ont. C.A.).
198 *R. v. Omar*, 2007 ONCA 117, 218 C.C.C. (3d) 242 at para. 31.
199 *R. v. S.(R.D.)*, [1997] 3 S.C.R. 484 at paras. 111-112.
200 R.S.C. 1985, c. J-1.

then decide to conduct a formal inquiry. Section 63(1) of the Act requires that a formal inquiry be held without any of these intermediate steps if the complaint is made by a provincial Attorney General or the federal Minister of Justice. The Federal Court of Appeal has upheld this as consistent with judicial independence even though the Attorney General or Minister may also effectively be a litigant in the case in question.[201]

The CJC is chaired by the Chief Justice of Canada and consists of the chief justice and associate chief justices of each superior court or branch or division thereof throughout Canada, as well as the senior judges in the courts of the territories. Section 60 of the Act defines the objectives of the CJC as being to promote efficiency and uniformity, and to improve the quality of judicial service in all superior courts of Canada. The CJC has the power under section 63 to investigate complaints by members of the public or by a member of the Council itself but, as noted above, it must conduct an inquiry if the Minister of Justice or the Attorney General of a province requests one. After the investigation or inquiry, which may include a request for a response from the judge, the CJC can make recommendations, ranging from the removal of the judge from office to delivery of a reprimand or a dismissal of the complaint.

Does the current Canadian Judicial Council (CJC) process sufficiently respect judicial independence? The fact that the CJC is composed of judges and not members of the executive or legislative branches of government satisfies some of the more formal requirements of judicial independence. However, it is important to go beyond formal requirements to ensure that, substantively, every judge is able to exercise judicial independence when making difficult decisions in often tense environments. There is a reasonable possibility some judges may see the disciplinary power of the CJC as being akin to a "watchdog" that second guesses difficult judicial decisions. Fear of such a watchdog is incompatible with a full and robust exercise of judicial independence.

An instructive case bearing on these very issues involved a long "biker gang" trial in Quebec. In the middle of the trial, the judge recused himself after he was reprimanded by the CJC for insulting one of the accused's lawyers at an earlier bail hearing. [202] The CJC's disciplinary decision was made available to a press reporter before the judge had received official notification of it. The judge took the position that, as a result of the reprimand, he had lost his moral authority to preside over the trial. A mistrial was eventually declared. A 15-week jury trial that had heard 113 witnesses had to be aborted. The judge's recusal then became the subject of a complaint by the Attorney General of Quebec to the CJC. A formal inquiry found that the judge's recusal was "improper" and that the reason he gave for recusing himself "…was not a valid reason for withdrawal

---

201 *Cosgrove v. Canadian Judicial Council*, 2007 FCA 103, 279 D.L.R. (4th) 352 at para. 51. This decision effectively recognizes that the historic mandate of the Attorney General to safeguard the integrity of the Justice system is not incompatible with his or her ultimate responsibility for the conduct of criminal prosecutions. The unique role played by the Attorney General is discussed elsewhere in this volume.

202 *R. v. Beauchamp*, [2002] R.J.Q. 2071, 4 C.R. (6th) 318 (Que. S.C.).

from the case."[203] The inquiry, undertaken by a panel of the CJC, found that the judge had failed in the execution of his office, but that this failure did not constitute grounds to recommend his removal from his office. The results of the panel's inquiry then came before the full CJC. The full CJC agreed that the judge should not be removed but disagreed with the inquiry's finding of impropriety. It stated: "Except where a judge has been guilty of bad faith or abuse of office, a discretionary judicial decision cannot form the basis for any of the kinds of misconduct, or failure or incompatibility in due execution of office…. Exercise of a judicial discretion is at the heart of judicial independence."[204] The CJC also articulated some limits on complaints by Attorneys General under section 63(1) of the *Judges Act*.

The CJC should continue to be sensitive to, and be seen to be sensitive to, the difficult position of trial judges who must aggressively manage long criminal trials. It should avoid fostering a concern that its operations threaten judicial independence, particularly in relation to the management of trials. One change that might reduce this concern lies in the composition of the Council. At present, membership in the CJC is limited to chief justices and associate chief justices. Historically, the chief justice was seen as the first among equals. The opinion of a chief justice, then as now, is of no greater weight than that of a puisne judge of the same court. As the number of judges has expanded in recent years, the administrative role of chief justices and associate chief justices has grown. The increase in administration includes additional and serious responsibilities, such as dealing with space requirements, budget allocations and court assignments, to name only a few. As a result, chief justices have become more distant from the other members of the court. Increased responsibility has also added more power to the office of chief justice. The result is a growing perception of what might be described as an "employer-employee" relationship in the courts.

The employer-employee characterization is not apt because a chief justice has no power of suspension or termination. Such powers would be inconsistent with the independence of each judge, even though the chief justice is a judge and not part of the executive or legislature. Chief justices do, however, have responsibility for assigning cases and for approving attendance at conferences, sabbaticals and other like activities, including service on public inquiries. Not surprisingly, some judges may see the chief justice as their "boss" in the real sense and not want to be adverse in interest. In truth, however, striving to please the "boss" threatens judicial independence.

There is merit in making all superior court judges eligible to serve as Council members, not merely as members of subcommittees. Professor Martin L.

---

203 Report of the Canadian Judicial Council to the Minister of Justice of Canada under ss. 65(1) of the *Judges Act* concerning Mr. Justice Jean-Guy Boilard of the Superior Court of Quebec (December 19, 2003), p. 1, online: Canadian Judicial Council <http://www.cjc-ccm.gc.ca/cmslib/general/conduct_inq_boilard_ReportIC_200312_en.pdf> (accessed December 5, 2008) [Canadian Judicial Council Report on Mr. Justice Boilard].

204 Canadian Judicial Council Report on Mr. Justice Boilard, p. 2, quoted with approval in *Cosgrove v. Canada (Attorney General)*, 2008 FC 941, 331 F.T.R. 271 at para. 15.

Friedland has argued that "…it would be desirable to involve puisne [regular, as opposed to chief] judges in discipline matters….To involve them in discipline would give them a greater stake in the process and would ensure that it is not solely the chief justices who are making the decisions."[205] This would allow puisne judges to participate in the critical initial decisions about whether complaints merit a formal public inquiry.[206] It would also allow puisne judges to take part in deciding whether to accept the findings and recommendations of inquiries.

Members of the CJC could be elected by members of their courts and serve a fixed term, to allow for rotation of members. To maintain continuity, the Chief Justice of Canada should remain the permanent Chairperson, as is the case at present. Along with a reaffirmation by the CJC of the centrality to judicial independence of judicial discretion and of the immunity of such discretionary decisions from disciplinary oversight, such changes to the structure and composition of the CJC would remove any alleged "chilling effect" that might otherwise result from the CJC's disciplinary powers. This "chilling effect" would no longer serve as an excuse for judges to fail to discharge their duty to act decisively and authoritatively in controlling the process in their court rooms.

Another change in the procedures of the CJC that would mitigate concerns that the hearing of complaints could impinge on judicial independence is the repeal of section 63(1) of the *Judges Act*. As discussed above, this provision requires a formal and public inquiry if a provincial Attorney General or the federal Minister of Justice lodges a complaint about a judge. The section 63(1) procedure short-circuits many intermediate steps that are available to deal with complaints that are made under section 63(2) of the Act. Section 63(1) has been the source of controversy[207] and *Charter* challenge on the basis of alleged inconsistency with judicial independence. There is no evidence that the procedure has been abused or exercised in a manner inconsistent with the Attorney General's obligations to act in the public interest.[208] Without considering the merits of the *Charter* issue, which will be resolved finally by the courts, section 63(1) is, in the Commission's view, in conflict with the spirit of full judicial independence. Section 63(1) allows one side to a dispute, provincial or federal attorneys general who may prosecute terrorism cases, to trigger a very formal and public process that can lead to

---

205 M.L. Friedland, *A Place Apart: Judicial Independence and Accountability in Canada* (Ottawa: Canadian Judicial Council, 1995), p. 138 [Friedland, *A Place Apart*].

206 A report commissioned by the Canadian Judicial Council recommended that while *puisne* judges should be allowed to serve on subcommittees, they should not serve on committees. With respect to the Judicial Conduct committee, the reason given was "…that it would not be appropriate for individual *puisne* judges to have [the authority to resolve complaints] in respect of complaints about other *puisne* judges": *The Way Forward: Final Report of the Special Committee on Future Directions to the Canadian Judicial Council* (2002), p.27, online: Canadian Judicial Council <http://www.cjc-ccm.gc.ca/cmslib/general/news_pub_other_FuturesReport_20021129_en.pdf> (accessed December 3, 2008).

207 Professor Friedland recommended that the ability of provincial Attorneys General to initiate an inquiry under s. 63(1) be removed: Friedland, *A Place Apart*, p. 139. Provincial Attorneys General conduct the vast majority of criminal prosecutions, but in the terrorism context, the federal Attorney General will frequently be the prosecution: see Chapter III.

208 Since 1977, there have been seven requests by an Attorney General for an inquiry under s. 63(1). Four resulted in a recommendation that the judge in question not be removed, two resulted in the judge's resignation before the inquiry started and one resulted in the judge's resignation after the inquiry recommended that the judge be removed from office: *Cosgrove v. Canadian Judicial Council*, 2007 FCA 103, 279 D.L.R. (4th) 352 at para. 40.

a recommendation that a judge be removed from office. Section 63(1) is not necessary because provincial and federal attorneys general can bring complaints like anyone else under section 63(2). Complaints under section 63(2), especially when supported by an Attorney General, would be considered seriously. They would, however, be subject to a process that is designed to resolve complaints in a much more summary and less public manner and that reserves the formal inquiry process as the last step of the complaint resolution process.

There are many reasons for the type of prolonged trials that create the danger of rendering some terrorism prosecutions unmanageable. A variety of other remedies relating to matters such as disclosure and pre-trial motions are necessary and are examined elsewhere in this chapter. No single measure can eliminate overly long trials. In some cases, such as the Air India trial, the very nature of the subject matter will require a long trial. Nevertheless, the control that judges exercise over the proceedings before them is a key factor in helping long trials to proceed fairly and efficiently. Terrorism prosecutions present special challenges in part because the stakes are so high. Both the prosecutor and the accused may engage in unnecessary tactics for a variety of reasons, ranging from extreme caution and adversarialism to outright attempts (by defence counsel) to sabotage the prosecution. Such tactics can only be controlled by a strong and independent judge. Although the suggestions advanced in the present discussion can be helpful in removing perceived obstacles to the exercise of judicial independence, in the end the issue comes down to judges' willingness to accept – and exercise with courage and integrity – the responsibility implicit in their role. Even if it means exercising powers that will be unpopular with some or all litigants and the public, or making decisions that run a risk of an appeal or a complaint to the Canadian Judicial Council, judges must remain in control of trials. Judicial independence is a fundamental part of our constitution. When managing terrorism prosecutions, judges must appreciate the role of judicial independence and act accordingly.

9.3.6 Pre-trial Motions

Much of the delay in a long trial occurs at the pre-trial stage. Ontario Court of Appeal Justice Michael Moldaver once described long criminal trials as a "… cancer on our criminal justice system" that posed a threat to its very existence.[209] He attributed long trials largely to the increasing length of the pre-trial phase, calling pre-trial motions "…this country's greatest growth industry."[210] The 2006 Ontario Superior Court Report agreed with Justice Moldaver, adding that pre-trial applications are "…the greatest reason why trials last longer than anticipated."[211]

Delays caused by pre-trial applications threaten the viability of terrorism trials. It is here that the greatest need to introduce efficiencies to the trial process arises. No legislative amendment is required to streamline pre-trial applications.

---

209 Moldaver Article on Long Criminal Trials at 316.
210 Moldaver Article on Long Criminal Trials at 319.
211 Ontario Superior Court Report on Criminal Trials, para. 307.

As discussed earlier, much of the solution can be found with the judge hearing the applications. A judge should not be afraid to control the courtroom – including taking control of the pre-trial process and establishing ground rules and deadlines for bringing applications.

Wright and Code recommended that all pre-trial applications be subject to the following rules:

- that all motions be in writing;
- that they be served on opposing counsel with two weeks notice; and
- that any defence to a motion be served in writing no later than one week before its presentation.[212]

The trial judge, appointed early in the process, should hear most pre-trial applications. As noted earlier, the Commission recommends that trial judges be authorized to handle applications under section 38 of the *Canada Evidence Act*. In fact, the trial judge should be the only judge to hear motions that are central to the case. Since only the trial judge can decide constitutional issues, having the trial judge appointed early also allows the early determination of those issues. In addition, questions of admissibility of evidence are so central to the case that they should not be heard by any judge but the trial judge. Such an approach also reinforces the notion that the responsibility of ensuring that the case comes to trial must be that of the trial judge.

There may be a few situations, however, where it is more appropriate for another judge to decide pre-trial motions. For example, the following pre-trial matters might be handled by a judge other than the trial judge:

- Rowbotham and Fisher-type applications;
- judicial interim release;
- plea discussion negotiations and guilty pleas (unless all accused plead guilty); and
- related investigative hearings.

In the Air India case, at least three judges heard motions besides trial judge Justice Josephson. Having such motions heard by a single judge other than the trial judge would promote continuity in decisions about the case and would make it much more likely that the judge hearing those motions would have a sound knowledge of the case. However, appointing a single judge to hear all motions that are not heard by the trial judge does risk setting up a second centre of power in the trial, which may detract from the authority of the trial judge.

Some groups have called for a "case management" judge to handle many of the pre-trial motions that the Commission recommends be handled by a trial

---

212 Wright and Code Report on Air India Trial, Part II, p. 8.

judge who has been appointed sufficiently early in the trial process. The Federal/Provincial/Territorial Working Group on Criminal Procedure, for example, recently called for the nomination of a "trial management judge" as part of the "exceptional trial procedure" that would come into play in a mega-trial.[213] The 2004 Steering Committee Report called for appointing a special "case management judge" to share the workload of the trial judge in mega-cases. This judge would have the same powers as the trial judge, and both judges would have the same status.[214] The Steering Committee recommended that the case management judge would be given authority to do the following:

- Consider all the issues relating to disclosure and make orders, particularly on the content and format of the disclosure and on its scheduling;
- Rule on bail applications and review of bail conditions;
- Rule on issues relating to funding for defence counsel, witnesses or jury members ...;
- Permit, where necessary, access to proceeds of crime;
- Rule on applications for severance ...;
- Rule on preliminary issues involving the presentation of evidence, including:
  - Admissibility of evidence;
  - *Charter* questions;
  - Requests of the *R. v. Corbett* type (regarding the exclusion of past convictions from the evidence);
  - Expert status;
- Fix deadlines and ask the parties to report on the progress of the file;
- Invite the parties to identify the issues, keeping in mind that the accused cannot be forced to make admissions ...;
- Put admissions made by the parties in the file.[215]

The Steering Committee recommended that the case management judge act as a facilitator for any negotiations between the prosecution and the defence – for example, about potential pleas and stays of prosecution. This was because "… the trial judge must refrain from participating in any such discussions."[216] The case management judge would serve as a mediator in negotiations regarding potential pleas by the accused and potential stays of certain charges by the Crown. The Steering Committee also recommended authorizing the case management judge, in certain circumstances, to hear guilty pleas and pass sentence.[217]

---

213 F/P/T Working Group Proposals on Mega-Trials, pp. 6-9.
214 Steering Committee Report on Mega trials, s. 4.2.1.
215 Steering Committee Report on Mega trials, s. 4.2.3.
216 Steering Committee Report on Mega trials, s. 4.2.6.
217 Steering Committee Report on Mega trials, s. 4.2.6.

In addition, the Steering Committee recommended that "…motions on matters filed during the trial … be referred to the management judge when they deal with matters completely separate from the evidence, or where a ruling from the management judge may need to be reopened in light of new facts or exceptional circumstances."[218] As well, once the case is in order and ready to go to trial, the case management judge would give the trial judge a report containing rulings on preliminary motions, orders about the disclosure of evidence, admissions made by the parties and issues identified by the parties.[219]

Some provinces already use case management judges and pre-trial judges to ensure efficiency in managing the pre-trial process.[220] The Steering Committee's recommendations would remove disparities among the provinces. The recommendations would ensure that many more pre-trial applications could be heard by a judge other than the trial judge, freeing the trial judge to attend to trial issues exclusively. In particular, the recommendations would allow for another judge to hear certain applications that are not appropriate for the trial judge to hear. The recommendations would also ensure that a single judge is responsible for every related application that is not to be heard by the trial judge. Finally, the 2004 Steering Committee Report's recommendations would force parties to bring their applications before the case management judge during the pre-trial phase or run the risk of having their late applications refused.[221]

Forcing parties to bring all or most of their applications during the pre-trial phase would represent a significant departure from the existing practice in most provinces and may not be advisable, particularly when it may not be possible for counsel (both defence and prosecutor) to identify in advance all the applications that should be brought. Good preparation and communication among counsel will provide some certainty, but it is impossible to script litigation in the way envisaged by the 2004 Steering Committee Report.

Leaving aside the merits of the proposals for non-terror cases, the Steering Committee proposals do not take into account the unique challenges of terrorism prosecutions. As discussed earlier, terrorism prosecutions are less likely than many other cases to be resolved by plea negotiations. Issues of disclosure, including whether secret intelligence will be disclosed to the accused under section 38 of the *Canada Evidence Act*, will play an important and sometimes critical role in terrorism prosecutions. The unique demands of disclosure in terrorism prosecutions may result in late disclosure issues that should be resolved by the trial judge. The trial judge must be able to reconcile the competing needs for disclosure and secrecy in a terrorism prosecution and revisit disclosure orders as the trial evolves. Remedies for disclosure violations may be best decided at the end of the case by the trial judge, as would have

---

218 Steering Committee Report on Mega trials, s. 4.2.6.

219 Steering Committee Report on Mega trials, s. 4.2.4.

220 Background Dossier For Term of Reference (b)(vi), p. 41. See, for example, the pre-trial recommendations of the Ontario Superior Court Report on Criminal Trials as well as the "management" and "facilitation" conferences for penal and criminal cases in Quebec.

221 Steering Committee Report on Mega trials, s. 4.2.3.

occurred in the Air India case but for the acquittals. These distinctive traits of terrorism trials all suggest that a competent, experienced and committed trial judge with the powers to make decisions about the broadest range of pre-trial matters should be appointed early on in a terrorism prosecution. Such early appointment should largely eliminate the need to bring another judge (except in the case of certain pre-trial motions described earlier) into a terrorism prosecution, even if the case management judge recommended in the 2004 Steering Committee Report is available.

Relying on a single trial judge to "case manage" a terrorism prosecution would avoid the need for legislative amendments to empower pre-trial management judges or to allow the parties or the Chief Justice to identify when a prosecution would be sufficiently complex to require the appointment of a case management judge. Moreover, relying on a single judge avoids the possibility of parties attempting to ask the trial judge to re-open earlier decisions of the pre-trial management judge.[222] It is simpler and more efficient to appoint the trial judge at an early stage. The proposed authority of the trial judge to re-visit any non-disclosure orders made under section 38 of the *Canada Evidence Act* would also help to ensure fairness towards the accused if developments in the trial make it necessary to disclose national security material that has previously been withheld. Whatever the merits of a pre-trial management judge may be in non-terrorism prosecutions, a matter that is in any event beyond the Commission's mandate, the challenges of terrorism prosecutions require that the trial judge firmly manage most aspects of the trial at the earliest possible opportunity. In principle, divided responsibilities and accountability should be avoided. Someone should be in charge. In a terrorism prosecution, the trial judge is that person.

9.3.7 Pre-trial Conferences

Section 625.1 of the *Criminal Code* provides the authority for pre-trial conferences. These are meant to promote a fair and expeditious trial and constitute one of the first official meetings between Crown and defence counsel. Pre-trial conferences

---

222 Although he favoured the two-judge model because the single judge model was "administratively rigid," Code conceded that "…educating two separate judges about one case is more resource intensive and creates some risk that the trial judge will disagree with the pre-trial judge's rulings and will reverse them if persuaded that something material has changed between the pre-trial and the trial. Only the judge who makes the pre-trial ruling really knows whether some change in circumstances would have been material to his or her original decision. Having two separate judges will inevitably encourage attempts to revisit earlier rulings. Furthermore, assigning the case at an early stage to one judge, who must both manage the case prior to trial and then try it (the one-judge model found in the English rules), encourages that judge to take ownership of the case, work diligently to either resolve it or shorten it, and take responsibility for the efficient management of his or her overall caseload": Code Article on Mega Trial Phenomenon at 457-458. On the English approach, which gives the trial judge extensive powers of active case management, including the power to decide and if necessary revise non-disclosure orders on the basis of public interest immunity, see Code Article on Mega Trial Phenomenon at 440-445; Roach Paper on Terrorism Prosecutions, pp. 260-269. Roach also notes that trial judges in Australia and the United States have robust case management powers, including the ability to make decisions about whether secret intelligence must be disclosed to the accused or can be disclosed in a modified form.

are mandatory in jury trials. In other trials, Crown or defence counsel may apply to the court for a pre-trial conference, or the court may order one on its own motion.

The pre-trial conference is often the ideal forum for discussions between counsel and the judge on matters such as disclosure, including disclosure involving section 38 of the *Canada Evidence Act*, plea bargaining, choice of mode of trial and length of trial, admissions of fact, *Charter* applications and other pre-trial motions, including the rules for the presentation of the motions.[223] Efficient and early discussions on these issues, combined with the willingness of counsel to compromise (and the authority to do so), can narrow the issues to be addressed at trial and provide a more efficient pre-trial and trial.

However, in many jurisdictions, counsel fail to take pre-trial conferences seriously,[224] if they even bother to attend them at all. Counsel who do attend often do so unprepared and without instructions from their clients, or they may send junior counsel with no knowledge of the file and no authority to make decisions or compromises.[225] In addition, the judge who presides at the pre-trial conference, if not the trial judge, may essentially be powerless to make binding orders on critical matters such as disclosure.[226] Such pre-trial conferences serve no useful purpose.

The 2006 Ontario Superior Court Report recognized that pre-trial conferences were not being taken seriously, were not being used to their full potential and did not fulfill their role as case management tools. The Report responded with a series of recommendations which set out proposed obligations for counsel and the matters to be covered.[227] The goal of these recommendations was to create a pre-trial conference system where counsel would study the case before the pre-trial conference and make binding commitments about various pre-trial and trial issues, including pre-trial applications that they intended to present and rules for their presentation.

The 2008 F/P/T Working Group Proposals also called for an enhanced pre-trial conference procedure, recommending a provision in the *Criminal Code* similar to section 536.4, which provides for pre-hearing conferences in the context of preliminary inquiries.[228] Section 536.4 contemplates meetings to identify the issues that require the calling of evidence, which witnesses must be heard, and their needs and circumstances. The section seeks to encourage the parties to make decisions to promote a fair and expeditious process.[229] Lesage and Code commented, however, that pre-hearing conferences are not being used effectively in preliminary inquiries because of the inability of the judges to make

---

223 Ontario Superior Court Report on Criminal Trials, paras. 197, 208.
224 Ontario Superior Court Report on Criminal Trials, para. 154.
225 Ontario Superior Court Report on Criminal Trials, paras. 155-156, 158-159.
226 *R. v. S.(S.S.)* (1999), 136 C.C.C. (3d) 477 (Ont. S.C.J.).
227 Ontario Superior Court Report on Criminal Trials, Chapter XVII: Compilation of Recommendations, Recommendations Regarding Pre-trial Conferences.
228 F/P/T Working Group Proposals on Mega-Trials, p. 8.
229 Allowance would have to be made for the differences between preliminary inquiries, which have limited objectives, and the conduct of actual criminal trials.

binding orders about the conduct of the proceeding.[230] This again underlines the importance of allowing the trial judge, not another judge, to conduct a pre-trial conference that produces binding deadlines and rulings.

As with the hearing of pre-trial motions, the trial judge should be involved in the pre-trial conference. The trial judge is fully invested in the case and will have a very direct interest in pressing for the case to proceed as efficiently as possible. This is not to say that the trial judge should try to force counsel to attend a pre-trial conference and dictate the issues to discuss. In some cases, it may be more appropriate for the judge to inform counsel that he or she is available for a pre-trial conference, but not to dictate the process, at least at that time. The main point, however, is that the trial judge should be in charge. Moreover, the trial judge should not be timid about managing the process to ensure that the case proceeds to verdict in an efficient and fair manner.

9.3.8 Reducing Delays and Re-litigation Caused by Severance Orders and Mistrials

Judges encouraging counsel to bring their applications early promises to expedite the trial process. Many pre-trial matters relating to issues such as disclosure, applications under section 38 of the *Canada Evidence Act*, the sufficiency of search warrants and perhaps even the admissibility of evidence could be made before trial. At the same time, it may be desirable for a terrorism prosecution of multiple accused, each perhaps with differing levels of involvement in the alleged terrorist activity, to be severed into smaller, more manageable prosecutions. There is also a possibility that a terrorism prosecution will end in a mistrial, as happened in *R. v. Ribic*, where the accused attempted to call secret evidence in the middle of the trial. Litigation and appeals in the Federal Court were necessary while the jury was kept waiting.[231] The jury agreed to the postponement, but the trial judge concluded at one point that, with more Federal Court proceedings pending, he must dismiss the jury and declare a mistrial.

At present, rulings rendered before a mistrial or before severance may have to be re-litigated before the judge of the severed or new trial.[232] Similarly, there is no provision in the *Criminal Code* to allow common pre-trial motions to be heard and decided in cases that were severed into separate prosecutions from the start. The present state of the law provides a perverse incentive for prosecutors to overload indictments with many accused and many charges and to resist severance in order to achieve efficiency and consistency in decisions about pre-trial motions. This deficiency in the *Criminal Code* persists despite the observations of many trial judges that severance of prosecutions with many

---

230 Lesage and Code Report on Large and Complex Criminal Case Procedures, p. 60.

231 For a case study of this prosecution, see Roach Paper on Terrorism Prosecutions, pp. 217-234.

232 Courts of Appeal in Canada appear to be divided about whether rulings of a trial judge before a mistrial continue to bind in the subsequent trial. See *R. v. Wu (J.J.)* (2002), 167 O.A.C. 141 at para. 25, suggesting that such rulings do bind. In contrast, see *R. v. Reashore*, 2002 NSCA 167, 170 C.C.C. (3d) 246 at para. 11, suggesting that such rulings may not be binding at the second trial.

accused and many charges is essential.[233] Although overloaded indictments and refusals to sever can make trials unwieldy, they ensure consistency in rulings about critical pre-trial matters such as the disclosure of intelligence and the admissibility of wiretaps, a consistency that might not be achieved with severed counts if essentially identical pre-trial motions are decided by different trial judges in separate trials.

MacFarlane argued that one of the causes of prolonged trials is overloaded indictments with too many accused and too many charges. He maintained that "…the Crown need not include every potential accused and every potential charge on the indictment."[234] Code agreed that "…there is no doubt that one cause of the mega trial phenomenon is over-loaded indictments with too many accused and too many counts." He added:

> One of the main disincentives to severance under our current legislative regime is that the Crown has a legitimate interest in obtaining single consistent rulings on the major procedural issues in a big case, such as disclosure, admissibility of evidence and any arguable Charter breaches. It makes no sense to litigate these issues repeatedly before separate judges at separate trials. As a result, under our current regime, the Crown understandably resists severance in order to consolidate the rulings before a single judge at a single trial. If the Criminal Code provided for an omnibus hearing of related motions from all related trials, severance of large cases into smaller cases would become a much more palatable remedy.[235]

It would not diminish the fairness of a subsequent trial to have the original ruling bind the judge of a new trial that occurs because of a severance or a mistrial. The accused and the Crown would have fully participated in the arguments leading to the ruling that was made before the severance or mistrial. The same is true if the cases are severed into separate, more manageable, prosecutions from the start and an omnibus hearing of common motions, with all accused represented, occurs before a single judge. In all these scenarios, the accused and the Crown will have been present and participated fully in the arguments leading to the ruling. Neither the accused nor the Crown can claim that the process is unfair, and neither should be allowed to re-litigate the ruling unless they can demonstrate a material change in circumstances. The same principle should apply after a mistrial.[236] Unless a material change in circumstances has occurred, the trial judge's rulings at the first trial should bind the parties at the second trial.

---

233 Justice Krindle, for example, has observed: "In my opinion, a trial of perhaps seven or eight accused would be difficult, but could be conducted, with the proper aids to the jury, without the jury's losing focus on the evidence and without the jury's losing the ability to isolate the evidence to the individuals and the issues. Beyond that number I believe that the interests of justice require severance": *R. v. Pangman*, 2000 MBQB 71, 149 Man. R. (2d) 68 at para. 30.

234 MacFarlane Paper on Terrorist Mega-Trials, p. 304.

235 Code Article on Mega Trial Phenomenon at 461-462.

236 However, this principle does not extend to a new trial ordered by an appeal court after it quashes a conviction. In such a case, the parties would have to agree to be bound by the pre-trial rulings made at the first trial.

Experienced counsel can agree to accept a ruling made before severance or a mistrial, but the preferred solution is to amend the *Criminal Code* to ensure that the ruling of the original trial judge is not affected by a severance order or a mistrial. The *Criminal Code* should also be amended to permit omnibus hearings on common motions in related prosecutions that have already been severed. That would mean, for example, that a pre-severance ruling on a *voir dire* about the constitutionality of the anti-terrorism legislation would bind the judge at the severed trial or that a ruling on the constitutionality of a wiretap at an omnibus hearing would bind trial judges in subsequent and separate prosecutions. The same should apply with rulings made before a mistrial is declared. The subsequent judge should be permitted to revisit rulings of the original judge only if materially different facts arise – as might occur, for example, because of continuing disclosure.

Finality is an important value in the criminal justice system. Litigants have no right to a second "kick at the can." The approach proposed above is fair because, in every case, the accused and the Crown are heard before rulings are made. Such an approach is efficient because it prevents re-litigation of the same issues in separate prosecutions. This approach is particularly important for prosecutions of alleged terrorist groups or cells because it allows the prosecution to be broken down and severed into manageable cases while still allowing common pre-trial issues to be resolved in a consistent manner.

It would be important to restrict interlocutory appeals of rulings made before a severance or mistrial, as well as those made at an omnibus motions hearing. Interlocutory appeals can be prevented by deeming the pre-severance, pre-mistrial or omnibus hearing rulings to be rulings of the trial judge in each prosecution. The accused and the Crown could still appeal these rulings, but only after the verdict, according to the standard appeal process of the *Criminal Code*.

Once severed trials conclude, there may be separate appeals of similar issues – for example, separate appeals of a pre-severance ruling about the constitutionality of a wiretap. In cases of separate appeals of similar issues, it should be possible for appellate courts to consolidate the appeals or grant standing to all the accused who would be affected by the appeal. Appeal courts regularly deal with problems created by multiple appeals of similar issues.[237]

The 2008 F/P/T Working Group Proposals suggest that more work needs to be done to ensure that the accused and the Crown are bound by decisions made before the prosecution is severed into separate trials and to deal with problems such as standing at appeals of issues decided before severance.[238]

---

237 See, for example, *Re McDonald and the Queen*, 21 C.C.C. (3d) 330 (Ont. C.A.).

238 F/P/T Working Group Proposals on Mega-Trials. The F/P/T Working Group suggests that "extensive examination" is still required "…to ensure that the joint hearing procedure as proposed would facilitate the conduct of mega-trials and not give rise to further complexity and additional procedural delays": p. 20, Proposal 8. At the same time, the Working Group accepts the principle that rulings should continue to bind after a mistrial is declared, absent fresh evidence or prejudice: p. 18, Proposal 7. It is difficult to comprehend the idea that the accused or Crown can claim prejudice from the application of the prior ruling unless there is fresh evidence demonstrating a material change in circumstances. It may promote unnecessary litigation and should be abandoned.

The Commission disagrees. The basic principles are relatively simple. First, decisions made before severance should bind separate trials conducted after severance. Second, omnibus hearings of common pre-trial motions should be allowed in related prosecutions. Section 645 of the *Criminal Code* should be amended to provide that decisions made on pre-trial motions before severance or at an omnibus hearing are deemed to be decisions of the trial judge in any subsequent prosecution. The decisions should be binding absent demonstration of a material change in circumstances. The accused and the Crown should have the right to appeal these rulings only according to regular appeal procedures that apply after the completion of the trial. Appellate courts should be able to manage problems raised by the possibility that one of the severed prosecutions may result in an appeal before the other prosecution is completed, given their control over matters of standing and intervention rights. An appellate decision that is rendered in one case before a related prosecution is completed should also be manageable. Trial judges regularly have to contend with changes in the law that are made in unrelated appeals and they can do so even if the appeal decision is made in a related case.

Prosecutions of suspected terrorist cells may involve many individuals with differing levels of involvement in a terrorist plot. Indeed, one group may be involved in multiple plots. The need for fairness and efficiency requires some prosecutions to be severed into separate and more manageable proceedings. At the same time, the problems of delay and re-litigation that will flow from sensible severance orders need to be remedied. This can be done by amendments to section 645 of the *Criminal Code*, as explained earlier, that will allow common pre-trial issues to be decided fairly and efficiently, and with some finality.

Recommendation 25:

To make terrorism prosecutions workable, the federal government should share the cost of major trials to ensure proper project management, victim services and adequate funding to attract experienced trial counsel who can make appropriate admissions of fact and exercise their other duties as officers of the court;

Recommendation 26:

The trial judge should be appointed as early as possible to manage the trial process, hear most pre-trial motions and make rulings; these rulings should not be subject to appeal before trial;

Recommendation 27:

The *Criminal Code* should be amended to ensure that pre-trial rulings by the trial judge continue to apply in the event that the prosecution subsequently ends in a mistrial or is severed into separate prosecutions. The only case in which rulings should not bind both the accused and the Crown should be if there is a demonstration of a material change in circumstances;

Recommendation 28:

The *Criminal Code* should be amended to allow omnibus hearings of common pre-trial motions in related but severed prosecutions. This will facilitate severing terrorism prosecutions that have common legal issues where separate trials would be fairer or more manageable. All accused in the related prosecutions should be represented at the omnibus hearing. Decisions made at omnibus hearings should bind the Crown and accused in subsequent trials unless a material change in circumstances can be demonstrated. Such rulings should be subject to appeal only after a verdict.

9.4 Disclosure

Chapter V reviewed the law relating to disclosure and production of relevant information to the accused. Canada has broad rights of disclosure which allow the accused to have access to information held by the Crown that is not clearly irrelevant to the case. The rationale of the rule is to protect the accused's right to a fair trial and to make full answer and defence, and to prevent miscarriages of justice. However, broad disclosure rights impose costs. There is evidence that they have damaged the relationship between the RCMP and CSIS because they limit the willingness of CSIS to give information to the RCMP and the willingness of the RCMP to receive it. Of greater relevance to the discussion in this chapter, broad disclosure rights place a significant burden on the trial process. Disclosure obligations in any terrorism prosecution are bound to be very onerous and will include many documents related to the police investigation, including non-privileged material relating to sources and agents. Disclosure may also involve intelligence material developed by CSIS or foreign agencies.

Chapter V examined the possibility of enacting legislation to limit the accused's rights to disclosure and production of material from third parties. Ultimately, it was concluded that such legislation would increase litigation, including *Charter* challenges, and that it would not help produce a workable relationship between intelligence and evidence. That said, it was also recommended that prosecutors be reminded in clear terms of their obligation to disclose only information that is relevant to the case, and that they need not disclose privileged material – notably material protected by informer privilege or a national security confidentiality claim. An indiscriminate "dump truck" approach to disclosure should be avoided. Early, well-organized and focused disclosure facilitates admissions of fact that will both shorten the trial process and permit the Crown and defence to plan their cases.

In a case the size of the Air India trial, early preparation is vital to ensure that the start of the trial is not delayed by late or incomplete disclosure. LeSage and Code noted that early disclosure requires police and prosecutors to collaborate closely to ensure a well-organized disclosure brief.[239] Fortunately, the Federal

---

239 Lesage and Code Report on Large and Complex Criminal Case Procedures, p. 44.

Prosecution Service Deskbook recognizes this important role of Crown counsel.[240] The policies in the Deskbook stress close cooperation between the police and the prosecutor with respect to the legal requirements and the organization of disclosure. One of the important roles of the new federal Director of Terrorism Prosecutions, a position whose creation is recommended in Chapter III, will be to assist investigators in developing a well-organized disclosure brief and giving legal advice to investigators about privileges that can protect information from disclosure. Close prosecutorial involvement in investigations is also required because section 83.24 of the *Criminal Code* requires the consent of the Attorney General to proceedings in respect of terrorism offences. Prosecutorial involvement should also facilitate informed discussions about the appropriate charges and consequent disclosure obligations. The precise extent of disclosure obligations depends on the nature of the charges that the accused faces.[241]

9.4.1 Electronic Disclosure

As noted earlier, much of the material disclosed in the Air India trial was disclosed electronically. This included the Crown brief (which was also disclosed in hard copy) and a second tier of material that might have been relevant to the defence but was not going to form a portion of the prosecution. A third tier of disclosure involved making large volumes of files available to the defence for manual inspection.

In his testimony, Code spoke about coming up with a practical procedure in the Air India trial and in future terrorism trials:

> The procedure can be devised, and there's nothing constitutional about proper procedure here or practical procedures here, so I think doing exactly what the B.C. prosecutors did in Air India and that we agreed with -- there was negotiation over this but it was all agreed with three tiers of disclosure. The most relevant the core Crown brief should be organized and produced in a hard copy in a Crown brief as it always has been. The second tier of what's recognized as relevant but the Crown's not relying on it, should be disclosed

240 The Federal Prosecution Service Deskbook provides that: "The most effective way of satisfying Crown counsel's ethical obligation to make full disclosure of the Crown's case is to be involved at an early stage and continue to be involved throughout the investigation. More than any other issue, the preparation of disclosure materials requires intensive cooperation between Crown counsel and the investigative agency, such that the responsibility should be viewed as a joint one. Crown counsel must give the investigative agency sufficient assistance and direction to ensure that the investigators produce a well-organized package that is as complete as possible and in a user-friendly format before charges are laid. The assistance provided should seek to enable the police to produce both excellent Crown briefs and complete disclosure packages for the defence." It goes on to note the role of the prosecutor in "…providing legal advice as to what material is privileged or non-disclosable for any other reason": The Federal Prosecution Service Deskbook, c. 54.3.1.3, online: Department of Justice Canada <http://www.justice.gc.ca/eng/dept-min/pub/fps-sfp/fpd/ch54.html> (accessed November 24, 2008).

241 See *R. v. Chaplin*, [1995] 1 S.C.R. 727, discussed in Chapter V.

> in CD ROM form after scanning it, and the third tier of the really marginal not clearly irrelevant material the Defence should have access to and on an undertaking and it's the Defence onus to ask for a copy of something that they find helpful. That's the first question about how can we come up with a practical procedure.[242]

Lawyers are increasingly computer literate. In terrorism trials that involve teams of lawyers, the inability of some members of those teams to deal with electronic disclosure should not be a problem since others will have sufficient computer skills. In addition, enhanced funding for counsel can be made contingent upon the legal team possessing sufficient technical abilities to manage electronic disclosure.

Although the trend of recent decisions affirms the validity of electronic disclosure, a legislative presumption in favour of electronic disclosure is necessary to ensure that trials are not derailed by unnecessary proceedings requesting paper disclosure.[243] The Hon. Bernard Grenier testified about the utility of electronic disclosure at mega–trials,[244] as did Bruce MacFarlane.[245] RCMP Assistant Commissioner Souccar advocated identifying and managing disclosure issues "…from day one of the investigation and not at the conclusion of the investigation."[246]

To encourage early disclosure and make voluminous disclosure more manageable, the *Criminal Code* should be amended to permit electronic disclosure and inspection of material by defence counsel in complex criminal cases that are designated as such by the presiding judge. This would allow a tiered approach to disclosure in appropriate cases, like that used in the Air India prosecution. As in that prosecution, defence counsel could in appropriate cases be required to attend at a secure location to inspect documents that, if disclosed, could harm national security. This inspection option is particularly important if, as required by the Supreme Court's recent decision in *Charkaoui*[247], material relating to prior CSIS investigations and surveillance of the accused and their associates is retained and the Crown agrees to make this material available to the accused. In such circumstances, defence counsel should be permitted

---

242 Testimony of Michael Code, vol. 88, December 4, 2007, p. 11373. See also Code's elaboration of a proposed disclosure process at pp. 11371-11373.

243 In *R. v. Chan* 2003 ABQB 759 (Q.B.) at para. 77, Sulyma J. referred to a June 2000 order by a Provincial Court judge, Maher J., that electronic disclosure was insufficient and that hard copy disclosure was required. This order dealt a considerable blow to the Crown in this case, as providing disclosure in hard copy to 34 co-accused was an enormous task. A stay of proceedings ultimately ended the Chan trial. At that time, the Crown was still in the process of providing hard copy disclosure to the co-accused: *R. v. Chan* 2003 ABQB 759. But for more recent decisions that recognize that electronic disclosure is sufficient see *R. v. Greer et al*, 2006 BCSC 1894 and *R. v. Piaskowski et al*, 2007 MBQB 68, [2007] 5 W.W.R. 323.

244 Testimony of Hon. Bernard Grenier, vol. 92, December 10, 2007, pp. 12179-12183.

245 Testimony of Bruce MacFarlane, vol. 78, November 19, 2007, pp. 9915-9917.

246 Testimony of Raf Souccar, vol. 78, November 19, 2007, p. 9983.

247 *Charkaoui v. Canada (Citizenship and Immigration)*, 2008 SCC 38, [2008] 2 S.C.R. 326.

to inspect such materials, but at a secure location where there are facilities for maintaining the confidentiality of the lawyer's work. Proposals have been made in England for similar limits on access to respond to concerns that disclosure could be misused, for example, to reveal the identity of those engaged in covert surveillance.[248]

In its Final Submissions, the Attorney General of Canada warned that even minor changes to the disclosure regime introduce complex and intractable issues about provincial jurisdiction and the ability of northern and remote communities to deal with the complexities of electronic disclosure.[249] In an age of widespread computer use, such concerns are overstated. In any event, the Attorney General of Canada retains the authority to prosecute terrorism offences and to change the province of venue of a terrorism trial, in the unlikely event that electronic disclosure would prove to be beyond the capabilities of a particular jurisdiction. In short, a provision could be added to the *Criminal Code* to allow the Crown to disclose evidence electronically.

9.4.2 Staged Disclosure

As discussed earlier, the Air India trial involved staged disclosure. The Crown brief was disclosed in paper format and electronically. Other relevant material was disclosed electronically, and defence counsel were permitted to inspect and obtain copies of further material, including sensitive material held by CSIS that was not clearly irrelevant. This type of inspection may be particularly valuable in cases like the Air India trial, where masses of wiretaps and other investigative materials exist, but are of limited relevance and will not be adduced as evidence. [250]

By all accounts, the staged approach to disclosure at the Air India trial was fair to all parties. It made the voluminous disclosure in this case more manageable. Although the Crown brief in the Air India trial was disclosed in paper as well as electronic format, paper disclosure may no longer be necessary. In these days of the ubiquitous computer, "…if the accused or counsel requires a hard copy of any of the material on the hard drive other than the video or audio portions it is a simple matter of printing it from the hard drive."[251] In appropriate cases, however, the Crown can make paper as well as electronic disclosure of the Crown brief.

Staged disclosure, including the possibility of simply making some material available for inspection, will be important in many terrorism cases. Relying on inspection allows the Crown to comply with even the broadest reading of *Stinchcombe* disclosure obligations while recognizing that disclosure of material of limited relevance at the outer peripheries of the *Stinchcombe* rule, even

---

248 David Ormerod, "Improving the Disclosure Regime," (2003) 7 International Journal of Evidence and Proof 102 at 127.
249 Final Submissions of the Attorney General of Canada, Vol. III, February 29, 2008, paras. 80-84.
250 *Criminal Code* wiretaps that are used as evidence must be transcribed: *Criminal Code*, s. 540(6).
251 *R. v. Greer et al*, 2006 BCSC 1894 at para. 32.

electronic disclosure, may sometimes be unworkable. Inspection requirements can be designed to alleviate legitimate security concerns that sensitive material that the Crown agrees can be disclosed to the accused's counsel not be used for other illegitimate purposes that may endanger sources and operatives. The accused should be given the option of inspecting material at a secure location, subject to compliance with security privileges that respect the need for solicitor-client confidentiality and the confidentiality of the lawyer's work product.

The trial judge should also set time limits for this staged disclosure and not allow disputes about disclosure to simmer or to delay the start of trial. In complex terrorism prosecutions, it is a reality that not all disclosure can occur at the same time. For this reason, the trial judge should "stay on top" of the disclosure process. This does not mean that the trial judge should attempt to read all the disclosure material or that counsel should be encouraged to dump all possible disclosure issues onto the trial judge. The trial judge should be able to expect that Crown counsel will discharge their ethical and legal obligations about disclosure, and that defence counsel will take the opportunity to inspect material of limited relevance, employ search engines to access electronically-disclosed materials, and justify requests for disclosure that go beyond the investigative file and raise peripheral matters.

Recommendation 29:

Electronic and staged disclosure should be used in terrorism prosecutions in order to make them more manageable. Disclosure should occur as follows:

Recommendation 30:

The Crown should be permitted to provide in electronic form any material on which it intends to rely and should have the discretion to provide paper copies of such material. If the Crown decides to use electronic disclosure, it must ensure that the defence has the necessary technical resources to use the resulting electronic database, including the appropriate software to allow annotation and searching;

Recommendation 31:

Material on which the Crown does not intend to rely but which is relevant should be produced in electronic format, and the necessary technical resources should be provided to allow the use of the resulting electronic database;

Recommendation 32:

The Crown should be able to disclose all other material that must be disclosed pursuant to *Stinchcombe* and *Charkaoui* by making it available to counsel for the accused for manual inspection. In cases where the disclosure involves sensitive material, the Crown should be able to require counsel for the accused to inspect the documents at a secure location with adequate provisions for maintaining the

confidentiality of the lawyer's work. Defence counsel should have a right to copy information but subject to complying with conditions to safeguard the information and to ensure that it is not used for improper purposes not connected with the trial;

Recommendation 33:

The trial judge should have the discretion to order full or partial paper disclosure where the interests of justice require; and

Recommendation 34:

The authority and procedures for electronic disclosure should be set out in the *Criminal Code* in order to prevent disputes about electronic disclosure**.**

9.4.3 Disclosure Issues Relating to Section 38 of the *Canada Evidence Act*

The undertakings signed by defence counsel in the Air India case permitted disclosure of sensitive material without bringing into play the Federal Court process currently required by section 38 of the *Canada Evidence Act*. This avoided what Code described as a "…document-by-document litigation model instead of a sensible negotiation model between counsel."[252] As noted earlier, counsel who signed an undertaking were allowed to view documents that the Crown might otherwise attempt to claim should be protected under section 38.

Code testified about the problems that he believed would arise if the parties had litigated claims under section 38. He stated that "…nobody wanted to do the section 38 procedure. It was an anathema." This was in part because of the procedure involved in educating a Federal Court judge about the case.[253] He testified further about hearing "…over and over again the legitimate concerns of the victims in these cases that the delays are unacceptable and ... we're just inviting delays with the current section 38 procedure."[254]

Two measures could facilitate addressing section 38 claims in future terrorism trials. The first, used in the Air India trial, has been described as a "band-aid" solution. It involved allowing defence counsel access to sensitive information on signing an undertaking. The second, discussed extensively in Chapter VII, is to move section 38 litigation out of the Federal Court and into the hands of Superior Court judges presiding at terrorism trials.

The first solution – the undertaking by defence counsel – worked well in the Air India trial. It was evidence of the commitment of experienced counsel to a manageable trial. It also worked because many of the incidents under

252 Testimony of Michael Code, vol. 88, December 4, 2007, p. 11385.
253 Testimony of Michael Code, vol. 88, December 4, 2007, pp. 11386-11387.
254 Testimony of Michael Code, vol. 88, December 4, 2007, p. 11391.

examination in the Air India trial were almost two decades old. Even if the documents being reviewed were originally highly classified, their age meant that there would be little danger of disclosing current CSIS intelligence, sources or operational methods.

This will likely not be the case with future terrorism trials. The classified information to which defence counsel will seek access will likely be current and may reveal existing operations, targets, sources and intelligence. Understandably, CSIS and the Attorney General would be reluctant to allow counsel who do not have security clearances to review some of these documents, and may challenge or prevent their release by using section 38.

Section 38 litigation may therefore be the only practical way to assess whether it is appropriate to disclose material that brings national security issues into play. Where litigation does become necessary, the Commission's proposed procedure for having section 38 applications heard by trial judges[255] would be much less disruptive than the current Federal Court procedure.

9.4.4 Late and Continuing Disclosure

The volume of materials to be disclosed can create a contest between providing early partial disclosure on time and providing complete disclosure later. Given that the accused are entitled to disclosure of all relevant evidence in the Crown's possession, the Crown's inclination may be to withhold disclosure until it has completed its review of all documents in the investigative file. In a perfect world, the Crown would be able to provide disclosure as of the date of the indictment, but this is often not the case, for a variety of reasons:

- The size of the investigative file may not permit a full review of the evidence to be completed in time;
- The accused may be charged very quickly if they are caught in the act;
- Evidence may be in the possession of numerous agencies and there may be delays in compiling it;
- Evidence may continue to be gathered after the charges are laid, especially if the investigation involves co-conspirators who have not yet been indicted;
- The Government may have to request other agencies to remove restrictions on the disclosure of information, but may not have received permission as of the date of the indictment; and
- The Crown may have exercised its discretion over the timing of disclosure to protect witnesses and sources.

---

255 See Chapter VII.

A complete review of the evidence before disclosure might cause delays, and ongoing investigations might make a complete one-time disclosure all but impossible in any event. As a result, it is necessary to strike a balance between timely and complete disclosure.

Late or incomplete disclosure has often been a significant issue in pre-trial applications during mega-trials. In the Air India trial, for example, Justice Josephson ruled on four occasions that the accused's disclosure rights had been violated as a result of lost or destroyed evidence[256] or late disclosure.[257] The extent of the Crown's duty to disclose and the timing of the disclosure required considerable judicial attention, involving 14 days of hearings and elaborate written submissions. At times, the discord that arose over disclosure strained the relationship between Crown and defence counsel.[258]

Because Justice Josephson ultimately acquitted Malik and Bagri, he did not need to decide the appropriate remedies for the various *Charter* breaches that involved late disclosure.[259] In other cases, *Charter* breaches flowing from late disclosure have given rise to a range of different remedies. In most cases, the remedies granted have been costs and adjournments. However, at times they have included the more drastic remedies of exclusion of evidence, mistrials and even stays of proceedings.[260] In *Chan*, late and incomplete disclosure led the accused to apply for a stay of proceedings on the grounds of unreasonable delay and breach of the right under section 11(b) of the *Charter* to be tried within a reasonable time.[261] The judge ordered the stay.

The lesson is clear. Timely and full (to the extent possible) disclosure is an indispensable element of the trial process. That said, there may be legitimate reasons for delays in disclosure, especially in complex terrorism prosecutions that may involve difficult issues of source and witness protection. The trial judge should be available to deal with disclosure disputes at the earliest juncture, and both the Crown and defence should come to the trial judge at the earliest opportunity with disputes over disclosure.

9.5 Issues at Trial

9.5.1 Inability of the Trial Judge to Continue

The Air India trial began on April 28, 2003, and continued until December 3, 2004 – a total of 217 trial days. Justice Josephson delivered his judgment on March 16, 2005.

---

256 *R. v. Malik, Bagri and Reyat*, 2002 BCSC 864; *R. v. Malik and Bagri*, 2004 BCSC 554, 119 C.R.R. (2d) 39.
257 *R. v. Malik, Bagri and Reyat*, 2002 BCSC 484; *R. v. Malik and Bagri*, 2004 BCSC 1309, 124 C.R.R. (2d) 270.
258 *R. v. Malik, Bagri and Reyat*, 2002 BCSC 484 at para. 24.
259 *R. v. Malik and Bagri*, 2005 BCSC 350 at para. 1250.
260 The remedial jurisprudence is examined in Kent Roach, *Constitutional Remedies in Canada* (Aurora: Canada Law Book, 1996), paras. 9.134-9.225.
261 *R. v. Chan*, 2003 ABQB 759.

In a jury trial, section 669.2 of the *Criminal Code* allows for a new judge to continue a jury trial if the first judge dies or becomes unable to continue. The new judge has the discretion to continue the trial or to recommence it as if no evidence had been taken.

The 2004 Barreau Committee Report and the 2004 Steering Committee Report both offered recommendations to deal with the death of the trial judge or the judge's inability otherwise to continue with a jury trial. Recognizing that this discretionary power to order a new jury trial could prove problematic, the Barreau Committee recommended that, when appointing a trial judge, the chief justice should also appoint an alternate judge. The alternate judge would keep abreast of the facts of the trial on a regular basis, such as through weekly summaries provided by the trial judge, and would be able to step in should the trial judge be unable to complete the trial.[262] The Barreau Committee argued that appointing a judge as an alternate would not prevent that judge from taking on other matters in the interim, since the responsibilities as an alternate would not fully occupy the judge. This arrangement would therefore not further strain judicial resources.[263] The 2004 Steering Committee Report, following a similar train of thought, spoke in favour of using a "case management judge" who could replace the trial judge if necessary,[264] as did the F/P/T Working Group.[265]

However, neither committee addressed the situation of a trial involving a judge alone. Section 669.2 of the *Criminal Code* requires that if a trial judge sitting alone becomes unable to complete the trial, the trial must begin anew. In the Air India trial, this did not occur, but there was a theoretical possibility that the trial judge could have become incapacitated. This would have led to the declaration of a mistrial. The proceedings would have had to commence anew in their entirety before another judge.

The 2008 F/P/T Working Group Proposals envisaged a trial management judge hearing a range of motions to assist the trial judge. If a mistrial occurred because of the inability of the trial judge to continue the trial or because of insufficient juror numbers, rulings and orders made by the management judge, as well as admissions by the parties, would continue to bind the parties. However, the parties would not be bound if prejudice to the accused could be demonstrated or if fresh evidence was introduced.[266]

There is a possibility a judge in a judge-alone terrorism trial would become unable to continue. However, appointing an alternate judge or a case management judge who could take over the trial may be an unnecessary response to a problem that at this point remains largely theoretical. That said, rulings made

262 Barreau Report on Mega-trials, s. 2.6.2.
263 Barreau Report on Mega-trials, s. 2.6.2.
264 Steering Committee Report on Mega trials, s. 4.2.6.
265 F/P/T Working Group Proposals on Mega-Trials, pp. 6-7.
266 F/P/T Working Group Proposals on Mega-Trials, p. 18. The Working Group noted the similar recommendation (recommendation 12) of the F/P/T Heads of Criminal Prosecutions on the Management of Mega-cases, adopted by the F/P/T Deputy Ministers Responsible for Justice, Ottawa, January 2004.

by the trial judge should continue to bind the parties if there is a mistrial unless a material change in circumstances can be demonstrated. This will at least preserve pre-trial rulings if a trial judge in a judge-alone terrorism prosecution becomes incapacitated. In many terrorism cases, the pre-trial rulings will take up most of the judge's time and thus the recommendation earlier that the pre-trial rulings of a judge shall continue to bind the parties will go a long way towards responding to the potential problems of the trial judge being incapacitated.

9.5.2 The Jury

Section 11(f) of the *Charter* guarantees the right to a trial by jury for offences carrying a maximum punishment of imprisonment for five years or more. With few exceptions, terrorism offences[267] qualify for jury trials on this basis. Some have suggested that juries are not well-suited to terrorism trials and that terrorism offences should be tried by a judge sitting alone. Trying terrorism offences before a three-judge panel sitting without a jury is a second option, one that the Commission's terms of reference require it to explore. However, both modes of trial would deprive the accused of the right to trial by jury. Doing so would attract constitutional scrutiny.

It is of course possible to avoid a constitutional issue by employing one of the following four measures:

- amending the *Charter*: Reaching the necessary political consensus for such an amendment would be extremely unlikely, so this possibility can be discounted;
- using the "notwithstanding clause" of the *Charter*[268]: It is unlikely that a government would rely on the notwithstanding clause and, in any event, the use of the notwithstanding clause would have to be renewed every five years;
- justifying the abolition of jury trials for terrorism trials as a reasonable limit on the section 11(f) *Charter* right to a jury trial
- that "…can be demonstrably justified in a free and democratic society"[269]: It will be very difficult to rely on section 1 of the *Charter* to justify abolishing jury trials because of the range of more proportionate responses that can be taken to improve the trial process and the jury system for long terrorism trials. There is also no evidence of widespread jury intimidation or juror partiality in Canada, circumstances that have been used to justify abolishing jury trials for terrorism trials in jurisdictions such as Ireland and Northern Ireland; or

---

267 Set out in Part II.1 of the *Criminal Code*.

268 *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act, 1982* (U.K.), 1982, c. 11, s. 33 [*Charter*].

269 *Charter*, s. 1. See also the test set out in *R. v. Oakes*, [1986] 1 S.C.R. 103.

- reducing the maximum penalty for terrorism offences to less than five years so that the right to trial by jury under section 11(f) would not apply: Given the gravity of most terrorism offences, a reduction of maximum penalties to less than five years imprisonment is simply not warranted.

As a result, the right to a jury trial is almost certain to remain a feature of terrorism trials. It is not feasible to override the *Charter* right to trial by jury or even to justify limits on the right, at least in the present circumstances in Canada.

Even if it was constitutionally possible to require that terrorism trials be held before either a single judge or a panel of three judges, it is not clear that it would be desirable to prevent trial by jury. In *R. v. Turpin*, Wilson J. spoke of the historical importance of the right to a jury trial:

> The right of the accused to receive a trial before a judge and jury of his or her peers is an important right which individuals have historically enjoyed in the common law world. The jury has often been praised as a bulwark of individual liberty. Sir William Blackstone, for example, called the jury "the glory of the English law" and "the most transcendent privilege which any subject can enjoy": Blackstone, Commentaries on the Laws of England (8th ed. 1778), vol. 3, at p. 379.
>
> The jury serves collective or social interests in addition to protecting the individual. The jury advances social purposes primarily by acting as a vehicle of public education and lending the weight of community standards to trial verdicts. Sir James Stephen underlined the collective interests served by trial by jury when he stated:
>
> > ... trial by jury interests large numbers of people in the administration of justice and makes them responsible for it. It is difficult to over-estimate the importance of this. It gives a degree of power and of popularity to the administration of justice which could hardly be derived from any other source
> >
> > J. Stephen, A History of the Criminal Law of England (1883), vol. I, at p. 573.
>
> In both its study paper (The Jury in Criminal Trials (1980), at pp. 5-17) and in its report to Parliament (The Jury (1982), at p. 5) the Law Reform Commission of Canada recognized that the jury functions both as a protection for the accused and as a public institution which benefits society in its educative and legitimizing roles.[270]

---

270 *R. v. Turpin*, [1989] 1 S.C.R. 1296 at 1309-1310.

The Quebec Barreau Committee report stated that "…this constitutional guarantee [of a right to a jury trial] serves to protect citizens against potential abusive or arbitrary procedures. It also serves to reassure citizens as to the quality and impartiality of our justice system."[271] The Barreau Committee concluded that the right to a jury trial should be maintained for all persons accused of a crime for which section 11(f) of the *Charter* guaranteed a right to a jury trial:

> An important part of the right to a fair trial is the right to be judged by a jury of peers, especially for the gravest crimes. The creation of special tribunals goes against the underlying principles of our legal tradition and our democratic values.... There is no reason justifying the setting aside of a right that is essential to the functioning of the judicial system in a democratic society.[272] [Translation]

At a conference in Ottawa in 2007, Justice Josephson spoke of his experience with the Air India trial and suggested that rulings in high profile terrorism trials have a better chance of winning public approval if delivered by juries rather than by judges: "I would have loved a jury trial to have made the factual findings in that case.... I think there's better acceptance of a verdict from a jury in the community, whether they convict or acquit."[273]

The issue then is not really about abolishing juries in terrorism trials. Instead, it is about how to make the trial environment less problematic for juries. Many of the recommendations discussed earlier are designed to make terrorism trials more efficient and more manageable. For example, encouraging the counsel to address matters through pre-trial motions, rather than motions during trial, will resolve many matters before the jury even begins sitting, and avoid the delay and the waste of jurors' time that would occur if these matters were brought up during the trial. Should motions that have to be heard outside of the jury's presence be required at trial, it is possible to schedule them in a manner that reduces the inconvenience to jurors who, after all, are providing a valuable public service. The Commission's recommendations, designed to facilitate the severance of terrorism prosecutions of large cells of alleged terrorists, should enable trials to be broken down into manageable portions while ensuring that common pre-trial motions are decided in a consistent, efficient and fair manner.

There is little doubt that a lengthy terrorism trial is likely to have a very negative financial impact on jurors. A review of the various provincial juror fee schemes reveals that many jurors can earn less, sometimes much less, than $100 per

---

271 Barreau Report on Mega-trials, s. 2.2, relying on the findings in *R. v. Born With A Tooth* (1993), 10 Alta. L.R. (3d) Q.B.

272 Barreau Report on Mega-trials, s. 2.2, relying on the findings in *Genest v. R.*, [1990] R.J.Q. 2387 (C.A.).

273 Jim Brown, "Jury trials preferable in terror cases, says Air India judge" *Winnipeg Free Press* (June 11, 2007), online: Winnipeg Free Press <http://www.winnipegfreepress.com/historic/32266404.html> (accessed July 8, 2009).

sitting day, depending on their province of residence.[274] In addition, the Canada Revenue Agency considers juror fees to be income for a service and thus taxable.[275]

More generous stipends should be available for jurors to avoid creating financial hardship if they sit on a lengthy case. This would also ensure that the jury represents a broad cross-section of the public, not merely those individuals whose employers are willing or able to continue paying them during prolonged jury duty. Although the setting of juror fees is a matter of provincial jurisdiction under section 92(14) of the *Constitution Act, 1867*, the federal government may have a role to play through cost-sharing agreements for particularly long terrorism trials.

Ultimately, to facilitate the work of juries and to minimize the personal difficulties that a lengthy commitment to a jury trial can cause, the trial process must become more efficient. Many of the measures proposed elsewhere in this volume are directed at doing just that. For example, allowing trial judges to decide matters under section 38 of the *Canada Evidence Act* and abolishing pre-trial appeals could prevent a situation like that in *R. v. Ribic*, where a jury was kept waiting and ultimately was dismissed because of lengthy litigation and appeals in the Federal Court. Measures recommended in this chapter should help significantly to shorten terrorist trials and make them more manageable. These measures include allowing omnibus hearings on common pre-trial motions and encouraging severance of terrorism prosecutions that might otherwise be characterized by multiple counts, multiple accused and multiple alleged terrorist plots. Trials such as the recently completed *Khawaja* prosecution tend to be heavily focused on pre-trial motions, with limited trial days. In *Khawaja*, the pre-trial motions on various matters took two years, while the actual trial – the time that a jury would be present if the case had been tried by jury – took only 27 days of hearings.[276] The early appointment of the trial judge and adequate funding for experienced counsel should also facilitate making reasonable admissions of fact. All these measures should help avoid the undesirable spectre of jury trials that last for years.

In summary, the following measures could lighten the load on juries:

- encouraging judges to be more assertive in controlling the trial – for example, by discouraging counsel from making needless or late motions, introducing unnecessary or excessive evidence or conducting excessive cross-examinations;

---

274 See the paper entitled "Juror Fees in Canada," appended as Appendix 1 to Background Dossier For Term of Reference (b)(vi).

275 Canada Revenue Agency, "Questions and answers about Other kinds of income", online: Canada Revenue Agency <http://www.cra-arc.gc.ca/tx/ndvdls/tpcs/ncm-tx/rtrn/cmpltng/rprtng-ncm/lns101-170/130/fq-eng.html> (accessed July 8, 2009).

276 *R. v. Khawaja*, [2008] O.J. No. 4244 (Sup. Ct.).

- providing sufficient funding to allow accused to retain experienced counsel and encouraging counsel to remember their obligations as officers of the court, both of which will promote a more efficient trial;
- encouraging more complete disclosure at the pre-trial stage so that counsel will not need to take time to review newly-disclosed material during the trial;
- encouraging severance where there are multiple accused and multiple counts, in order to reduce the length and complexity of trials;
- amending the law to ensure that decisions of the original pre-trial judge on pre-severance motions (the admissibility of wiretap evidence, for example) will not be re-litigated during the new trial that was created by the severance, and by allowing omnibus motions to be decided by one judge for common issues even when the prosecutions were severed from the start;
- facilitating the pre-trial resolution of motions;
- encouraging the use of pre-trial conferences to arrive at agreed statements of facts, admissions of fact and agreements on other trial management issues; and
- involving an efficient project management team in the pre-trial and trial processes.

9.5.2.1 Avoiding Mistrials Caused by Discharge of Jurors

During a jury trial, counsel and even the trial judge may be replaced without having to start the trial anew. However, jurors may not be replaced, and section 644(2) of the *Criminal Code* requires a minimum of 10 jurors for a valid verdict. If fewer than 10 jurors remain to deliberate after the evidence is heard, the trial judge must order a mistrial and begin the trial anew with a new jury.[277] Since jury trials begin with 12 jurors, this means that the judge may discharge at most two jurors. A discharge of three or more jurors results in a mistrial.[278] Jurors are chosen from the population at large and inquiries are generally not made about a juror's health at the start of the trial. Some jurors find the experience of sitting on a jury to be quite stressful, for a variety of reasons, and this can contribute to health problems. In contrast, a chief justice who assigns a trial judge to a particularly long trial can take steps to ensure that the judge is experienced and healthy. Thus there is a greater danger that jurors will become incapacitated during a terrorism trial than a judge.

The risk of a mistrial in a long trial is obvious. In a 2003 BC Supreme Court decision, Southin J. spoke of the need to make changes to the current jury system because of this:

---

277 The issue of mistrials because of too few jurors is discussed in detail in Background Dossier For Term of Reference (b)(vi), pp. 20-22.

278 Since 2002, s. 631(2.1) of the *Criminal Code* allows the trial judge to empanel up to 14 jurors at the time of jury selection. However, these alternates are excused at the start of the trial if they are not required at that time (s. 642.1(2)). The risk remains of a mistrial because of too few jurors at the stage of jury deliberation.

> I digress to note that on at least five occasions, the 21st May, 3rd June, 16th June, 11th July, and 25th July, this trial had to be adjourned because a juror was ill. Indeed, on the 25th July, two jurors were ill. The Criminal Code prescribes the minimum number of jurors who can give a verdict as ten. If the two jurors were too ill to continue and had been discharged and if a third juror had died suddenly on 29th July, this trial would have become a thing of naught. With the advent in recent years of very long trials, Parliament ought to enact a system in which more than twelve jurors shall be empanelled, but at the end of all the evidence only twelve, chosen in some manner, shall deliberate upon the evidence and return the verdict.[279]

Given the pressures that jurors may face in future terrorism trials of the length and complexity of the Air India trial, there is a substantial risk that more than two jurors will be discharged over the course of the trial, leading to a mistrial and the waste of much time. There also is a danger that unethical defence counsel may attempt to "rag the puck," hoping for such a mistrial.[280] Wholly apart from the additional stress and frustration for all parties – including the victims – that would flow from having to empanel a second jury and undergo a second trial, such a trial would impose enormous additional costs on the justice system. It could undermine the right of accused to be tried within a reasonable time and lead to a stay of proceedings. This in turn could (perhaps deservedly) cast the justice system in a very negative light.

Empanelling additional jurors might also prevent the need for adjournments when one of the jurors is temporarily unable to sit because of illness. In such cases, the trial judge could dismiss the ill juror and continue the trial before the remaining panel of jurors. Code noted that, at present, when jurors become sick during a long trial, "…the present statutory regime places great pressure on the trial judge to adjourn the trial, until the juror recovers, instead of simply replacing the sick juror with an 'alternate'. As a result, long trials become even longer."[281]

The Barreau Committee recommended increasing to 14 the number of jurors empanelled in a mega-trial.[282] Several witnesses before the Commission also

---

279 *R. v. Ho*, 2003 BCCA 663, 17 C.R. (6th) 223 at para. 6.

280 "An accused who has a weak defence on the merits, in a long complex case, may not agree to admissions or to a judge-alone trial because the risk of a s. 644(2) mistrial becomes part of the defence strategy. This kind of conduct is probably unethical but it introduces a completely arbitrary risk that is unacceptable and that needs to be removed from our justice system": Code Article on Mega Trial Phenomenon at 454.

281 Code Article on Mega Trial Phenomenon at 454.

282 Barreau Report on Mega-trials, s. 2.2. See also Testimony of Hon. Bernard Grenier, retired Justice of the Cour du Québec Criminal Division, who participated in the work of the Barreau Committee. He described this 14-juror approach, rather than 15 or 16 jurors, as "a suitable compromise": Testimony of Hon. Bernard Grenier, vol. 92, December 10, pp. 12157-12158; translation, original in French. See also Code Article on Mega Trial Phenomenon at 453, where the author states his support for introducing "alternate" jurors. Sections 642.1, 643 and 644(1.1) of the *Criminal Code* would have to be amended to allow a judge to empanel a jury of 14.

supported increasing the maximum number of jurors empanelled to hear a case,[283] generally suggesting a total of 14 or 16 jurors.[284] The Criminal Lawyers' Association proposed a system very similar to that suggested by the Barreau Committee: 14 jurors to hear the case, and a random system to discharge any excess jurors if more than 12 remain at the start of jury deliberations.[285]

On the other hand, the 2004 Steering Committee Report rejected increasing the maximum number of jurors and recommended instead that there be a "…specific and in-depth examination" of the issue of reducing the minimum number of jurors to 9 or 8, "…in particular, as regards potential constitutional implications."[286] The 2008 F/P/T Working Group Proposals called for swearing in up to 14 jurors, and reducing the minimum number required to deliberate to nine.[287]

Using any of these models, the judge would be able to discharge more jurors than at present and yet still prevent a mistrial. However, the model that involves reducing the number of jurors required to deliberate to fewer than 10 raises constitutional issues.[288] Allowing a lesser number of jurors to render a verdict might also raise concerns about how well the jury represents the community.[289] (However, as long as 10 jurors remain at the start of deliberations, it is worth considering allowing a verdict to stand even if one of those remaining 10 jurors becomes unable to complete the deliberation process.)

The better approach is simply to increase the maximum number of jurors. It avoids potential *Charter* issues and increases the likelihood that the jury will be seen as representing the community.

If judges are allowed to empanel additional jurors, there are two plausible models for choosing the jurors who would ultimately deliberate on the case if more than 12 jurors remain when deliberations begin. In the first model, all jurors believe from the outset of the trial that they are full jurors, but some may

---

283 Testimony of Ralph Steinberg, vol. 93, December 11, 2007, pp. 12316-12317; Testimony of Bruce MacFarlane, vol. 79, November 20, 2007, pp. 10041-10046. The Air India Victims' Families Association stated that "…(c)onsideration should be given to the provision of alternate jurors or reducing the number of jurors required to maintain the trial and deliver a verdict", but it did not provide any further detail or opinion on the matter: *Where is Justice?* AIVFA Final Written Submission, February 29, 2008, p. 168.

284 Bruce MacFarlane stated that, under federal American law, it is well established that up to and including six alternate jurors can be empanelled when a case is expected to be lengthy. He suggested that adopting this practice in Canada "…would be quite a jump from where we are right now" and that adding four extra jurors, as is done in the Victoria model in Australia, would be an acceptable compromise: Testimony of Bruce MacFarlane, vol. 78, November 19, 2007, p. 9905; Testimony of Bruce MacFarlane, vol. 79, November 20, 2007, pp. 10045-10046.

285 Submissions of the Criminal Lawyers' Association, February 2008, pp. 50-51 [Submissions of the Criminal Lawyers' Association].

286 Steering Committee Report on Mega trials, s. 5.3.

287 F/P/T/ Working Group Proposals on Mega-Trials, p. 15.

288 Testimony of Pierre Lapointe, vol. 94, December 12, 2007, pp. 12478-12479; Barreau Report on Mega-trials, s. 2.2. See also Testimony of Ralph Steinberg, vol. 93, December 11, 2007, p. 12316 and Code Article on Mega Trial Phenomenon at 452.

289 Code Article on Mega Trial Phenomenon at 452-453.

be removed by ballot as deliberations begin.[290] Balloting would not inevitably be necessary, since juror illness during a long trial could see the jury numbers reduced.

The second model involves distinguishing from the outset between regular and alternate jurors.[291] Alternate jurors would know that they would be called on to deliberate only if too few regular jurors remained when deliberations began.

The Commission prefers the balloting system, which should promote greater "ownership" of the case by all jurors. The "alternate" juror model might lead to the alternates not feeling as fully committed to paying attention at the trial, since there would be a good chance that they would not ultimately be involved in the jury deliberations.[292]

The Commission recommends authorizing the trial judge to empanel up to four additional jurors at the outset of the trial, bringing the possible number of jurors at the start of the trial to 16. This would permit the judge to discharge six jurors before it would be necessary to declare a mistrial (if the minimum number of jurors remains at 10). If more than 12 jurors remain at the start of deliberations, the 12 jurors who are to deliberate should be selected by ballot.

Empanelling additional jurors would of course raise costs and introduce additional logistical issues. Increasing to 16 the number of jurors was considered by the Quebec panel at Commission hearings to be something that would considerably increase jury management problems. This might be a price that must be paid. The disadvantages are easily outweighed by the many benefits of reducing the risk of a mistrial or having to adjourn a trial because a juror is sick. If more jurors are empanelled at the start, the trial judge can dismiss a sick juror in order to continue the trial in an efficient manner. Moreover, the trial judge could decide how many additional jurors would hear the case and would not have to empanel 16 jurors in every case.

9.5.3 Three-judge Panels

The Commission's terms of reference require it to analyze "…whether there is merit in having terrorism cases heard by a panel of three judges." The issue of a three-judge panel was raised in the Rae Report:

> The families' concerns also extend to the conduct of criminal trials in cases of this kind. Some have suggested that a panel of three judges would be more appropriate. While I have not suggested this as a specific question for the inquiry, it is certainly an issue worthy of study and discussion.[293]

---

290 Testimony of Bruce MacFarlane, vol. 78, November 19, 2007, p. 9906.
291 Testimony of Bruce MacFarlane, vol. 78, November 19, 2007, p. 9906.
292 Testimony of Bruce MacFarlane, vol. 79, November 20, 2007, p. 10047. See also Submissions of the Criminal Lawyers' Association, p. 51.
293 *Lessons to be Learned, p.* 4.

It is apparent that discussion of three-judge panels was intended to focus on their use within the existing common law model of adjudication. The call to consider a three-judge panel at the trial level is not to be misinterpreted as a call for an inquisitorial system. Any such change would profoundly alter the principles of the Canadian legal system. The terms of reference would certainly have made it clear if a consideration of shifting from a common law to an inquisitorial model of adjudication was to form part of the analysis.

The passage from the Rae Report quoted above leaves open three possible uses of a three-judge panel:

- to replace a judge sitting alone;
- to replace a judge sitting with a jury, leaving the jury to perform its traditional function; or
- to replace both judge and jury.

It is apparent that proposals for three-judge panels in terrorism cases are limited to cases that are not heard by a jury. It would not be practical or desirable for a three judge panel to sit with a jury. As a result, the discussion of three-judge panels here is restricted to considering whether they should replace trial by judge and jury or trial by judge alone.

Replacing judge and jury: Some foreign jurisdictions allow trials for terrorism offences to be heard without a jury even if the right to trial by jury is long-established and constitutionally protected. In the Republic of Ireland, the Special Criminal Court hears trials for numerous matters, including terrorism offences.[294] The Special Criminal Court sits as a three-judge panel with no jury, and verdicts are by majority vote.[295] Judge-alone trials, known as "Diplock"[296] courts, were used for terrorism trials in Northern Ireland after the right to a jury trial was suspended in 1973, in large part because of concerns about juror partiality and intimidation.[297] The authority to hold such non-jury trials continues under the *Justice and Security (Northern Ireland) Act, 2007*,[298] including in cases involving proscribed organizations or offences committed "…as a result of, in connection with or in response to religious or political hostility of one person or group of

---

294 *Offences against the State Act, 1939*, Ireland Statute No. 13/1939, online: Irish Statute Book <http://www.irishstatutebook.ie/ZZA13Y1939.html> (accessed November 20, 2008).

295 The Courts: Special Criminal Court, online: Ireland Courts Service <http://www.courts.ie/courts.ie/Library3.nsf/6556fea313d95d3180256a990052c571/41c06a30e5feda7b80256d870050508c?OpenDocument> (accessed November 20, 2008).

296 MacFarlane describes the origins of the "Diplock courts": "When the United Kingdom government imposed direct rule on Northern Ireland in 1972 following Bloody Sunday, it tried to steer towards a policy, known as "criminalization", of dealing with political violence through the criminal courts. It set up a commission chaired by Lord Diplock, a British law lord, to review criminal procedure, which recommended a number of security measures, including the introduction of single judge trials known as "Diplock" trials in place of the jury in cases of political violence": MacFarlane Paper on Terrorist Mega-Trials, pp. 174-175.

297 MacFarlane Paper on Terrorist Mega-Trials, pp. 174-175.

298 (N.I.), 2007, c. 6, s. 1.

persons towards another person or group of persons."[299] The evidence before the Commission makes it clear that one of the purposes of the three-judge panel in Ireland is to increase the level of safety of the judges themselves.

Another example of a three-judge panel without a jury was the *ad hoc* court created to hear the Lockerbie case. By agreement, the Libyan accused were tried in The Netherlands before a panel of three Scottish judges sitting without a jury. The Scottish Parliament had to enact a special provision to create the three-judge panel, allow it to hear the case in the absence of a jury, issue verdicts by majority vote and sit outside Scotland.[300] Bruce MacFarlane has commented on the dangers of *ad hoc* changes to the justice system to respond to horrific acts of terrorism, including the Lockerbie and Air India bombings.[301]

France uses jury trials for the gravest offences, but has also adopted a trial system without jury for terrorism trials.[302] *Le tribunal de grande instance de Paris* – the Tribunal of Paris – was granted a national competence for terrorism cases.[303] This led to the specialization of eight magistrates from the prosecution service and eight judges from the investigation service.[304] From this pool of magistrates and judges, a panel with one president and six assessors is assembled for each trial.[305] Verdicts are rendered by a majority vote.[306]

The constitutional difficulties that would arise if a three-judge panel were to replace trial by judge and jury are substantial. Furthermore, there is a long tradition of trust in the jury in the common law system. For these reasons alone, the jury trials should remain an option in terrorism cases unless compelling reasons can be provided to eliminate the jury.

This is not to deny that three-judge panels may have some attractive features. For example, the Hon. Ruth Krindle, a retired Manitoba Court of Queen's Bench judge, suggested in her testimony that three judges would probably move more expeditiously than a jury. However, there is no *certainty* that three judges would be significantly more efficient than a judge and jury. Indeed, it is possible that the need to retain the attention of a jury helps focus the efforts of both the Crown and the accused. Even informed speculation that a three-judge panel might be more efficient than a jury does not justify the procedural upheaval that introducing a three-judge panel would cause.

In his report prepared for the Commission, MacFarlane rejected the notion of a three-judge panel for several reasons:

---

299 (N.I.), 2007, c. 6, s. 1(6).
300 *The High Court of Justiciary (Proceedings in the Netherlands) (United Nations) Order 1998* (S.I. 1998 No. 2251), Arts. 3, 5.
301 MacFarlane Paper on Terrorist Mega-Trials, pp. 181-193.
302 French *Penal Code*, Art. 698-6(1).
303 French *Penal Code*, Art. 706-17.
304 Olivier Dutheillet de Lamothe, "French Legislation Against Terrorism: Constitutional Issues" (November 2006), pp. 6-7.
305 French *Penal Code*, Art. 698-6.
306 French *Penal Code*, Art. 698-6(3). This vote is tabulated through a secret ballot system, where each ballot is read in open court and then burned (Art. 358).

> In my view, replacement of a judge and jury with a panel of three judges in a terrorist case would, from a policy perspective, be ill-advised for several reasons.
>
> First, it seems to me that the conclusions of a panel would have to be unanimous on all essential issues of fact and law. Otherwise, almost by definition, a reasonable doubt exists in the case and an acquittal must be entered. In a jury trial, the issue of reasonable doubt is resolved through a unique process of group deliberation. Judges, however, have no such mandate, and would be entitled, in essence, to "vote" on the issue. Because the group deliberation and dynamic that is so important in jury fact-finding will not necessarily be present in a trial by a panel of professional judges, it seems to me that a bench trial could actually be a less effective fact-finding body than a jury of twelve randomly-selected jurors drawn from the general population.
>
> Second, the real challenge for future terrorist trials is . . . prolixity and complexity. Creation of a three judge bench trial is not responsive to that issue. Indeed, a bench trial simply raises new problems. . . . [I]n a lengthy trial a judicial panel could lose one of the judges just as easily as a jury could lose one of the jurors. What happens then? Do you proceed with just two judges? What do you do if the panel is reduced to one? At what stage do you declare a mistrial? Or do you "load up" at the front end with three judges and an alternate? In my view, few if any jurisdictions in Canada could afford the resource burden of routinely assigning four judges to hear terrorist trials.
>
> Finally, bench trials are ill-advised in Canada because they will raise significant issues of legitimacy. A panel of judges hearing a criminal case will be unique and without precedent in Canadian legal history. At the international level, terrorist cases would be seen as having been diverted out of the mainstream of Canadian trial procedure, and placed into the hands of a tribunal which has no parallel in Anglo-based criminal justice systems. Such a process would expose the tribunal to allegations of "show trial", as occurred in the Lockerbie experience, and may tend to diminish Canada's reputation for fair justice in the eyes of the international community.[307]

As discussed earlier, it would be extremely difficult to argue successfully that taking away the accused's right to a jury trial under section 11(f) of the *Charter* is a reasonable and demonstrably justified limit on the right. A court hearing

---

307 MacFarlane Paper on Terrorist Mega-Trials, p. 301.

such an argument would rightly be concerned that the state had not pursued other means of expediting terrorism trials that are less likely to diminish rights. Indeed, the simple expedient of increasing the number of alternate jurors has not been tried. The many reports and recommendations that have already been issued on the reforms needed to reduce the length of criminal trials would be cited as persuasive evidence that there are means to deal with the problem of long criminal trials short of taking away the right to trial by jury. Courts would also be aware that Canada, fortunately, has not suffered the history of juror intimidation and partiality found in places such as Northern Ireland. The remaining constitutional options, such as amending the *Charter*, adjusting maximum punishments for terrorism offences below five years so that the right to trial by jury does not apply, or using the notwithstanding clause, are simply not feasible.

Realistically, that only leaves consideration of the three-judge panel as a replacement for a judge sitting alone. In other words, the accused would have the ability to select either trial by jury or trial by a three-judge panel in terrorism cases. There are possible merits in three-judge panels here:

- "Three heads may be better than one" in a long, complex terrorism trial. The combined attention of three judges might ensure a more thorough and accurate understanding of the evidence. MacFarlane noted, for example, that "… [i]nternationally, trial by a panel of judges is considered desirable on the basis that a panel sitting together (usually three) would reduce the strain on a single judge, and the resulting decision would have greater credibility than a judge sitting alone";[308]

- The law recognizes terrorism as a special phenomenon in criminal justice, in terms of motive, purpose, potential penalties, and (until recently, when the authority to hold investigative hearings and make preventive arrests ended) investigative procedures. Arguably, the institutional structure for adjudication should also be adapted to respond to terrorism as an especially grave political or moral phenomenon. If nothing else, the allocation of extra judicial resources to terrorism trials would symbolize the state's recognition of terrorism as being uniquely hostile to Canadian values; and

- In the absence of a jury of fellow citizens, the public might have more confidence in a panel of judges, deliberating collectively on a verdict, than in a single judge, deciding alone without the benefit of a "sounding board" for some critical decisions (for example, on a matter of personal judgment such as assessing a witness's credibility). In the event of a controversial

308 MacFarlane Paper on Terrorist Mega-Trials, p. 250. See also Testimony of Michael Code, vol. 88, December 4, 2007, p. 11404.

> acquittal or conviction, the system of justice as a whole might be better protected from the corrosive effect of public criticism if a panel of judges, rather than a lone – and possibly overburdened – judge, reached the decision.

However, it is not clear that having three judges would reduce the risk of a mistrial, since one of them might become ill. Other questions remain to be resolved. How would the members of the panel be nominated, what rules of procedure would apply, and how would the panel's decisions be rendered about procedural questions, findings of law, findings of fact, credibility of witnesses, and ultimate findings about guilt? Although these procedural complexities are not insurmountable, they would make terrorism trials more complex and uncertain. Terrorism prosecutions are already difficult enough without having to work with novel and unprecedented institutions such as a three-judge trial panel. Although it can be argued that decisions rendered by three judges rather than one judge may inspire greater public confidence, even this is not a certainty, especially if one judge issues a dissent on a contentious issue. It would be difficult to force unanimity on judges who each enjoy the protections of judicial independence.

Code specifically raised in his testimony the difficulty posed by inconsistent findings of fact among panel members:

> At a trial level where the fundamental function of a trial court is fact-finding and . . . [the judges] agree on their verdict, you don't have a problem. You, in essence, end up with one set of reasons.
>
> But if they get to their verdict by different routes or if they've got a dissent, then I think you're into very, very serious difficulties because what you're going to have is ... a majority carrying out their [R. v. Sheppard[309]] duty to show the path by which they got to their fact-finding and a minority setting out their path by which they got to a different factual conclusion.[310]

The verdict of a judge sitting alone has the advantage of being clear and unequivocal. Divergent verdicts in a three-judge panel could cause serious problems. For example, a majority decision could lead to numerous appeals and further delays.

Ralph Steinberg, an experienced criminal lawyer, suggested that three-judge panels "…would add another layer of complexity that would just probably lengthen the duration of trials. I mean, if that proposal is directed toward one judge becoming incapacitated and causing a mistrial ... it may be an answer

---

309 2002 SCC 26, [2002] 1 S.C.R. 869.
310 Testimony of Michael Code, vol. 88, December 4, 2007, pp. 11401-11402.

to that but I don't think that that problem occurs with sufficient frequency to cause that kind of reform to be instituted."[311] Justice Krindle testified that, "… on a very practical level it would decimate any court to have three experienced trial judges [try a case]."[312] Indeed, a three-judge panel could place undue strain on already sparse judicial resources, especially in smaller provinces.[313] It could also generate pressure for appeals on matters in which the three-judge panel rendered a split decision.[314]

There are other reasons for rejecting three-judge panels for terrorism trials. Among the most important, introducing a three-judge panel would be inconsistent with the spirit of other Commission recommendations that move towards strengthening the role of Superior Court judges in non-jury trials. There is a need for one trial judge, not a panel of independent judges, to be in charge of managing the trial process. As well, there is no sound basis for believing that the verdict of the judge alone is any less valid than that to be rendered by a three-judge panel. The use of the three-judge panel might not make the trial shorter or more likely to come to a verdict. It therefore does not appear to be a certain solution to concerns about unduly lengthy trials.

Finally, the legitimacy of the novel institution of a three-judge panel might be called into question, especially if used only for terrorism trials. As MacFarlane suggested in his study for the Commission, Canada's reputation for fair justice in the eyes of the international community may be diminished if terrorist cases are seen as having been diverted from the ordinary system of justice.[315] Attempts to devise new courts to deal with national security matters have not generally been successful.[316]

9.5.4 Mandatory Jury Trials

At present, there are two trial options for terrorism trials – trial by judge alone or trial by judge and jury. Is there any compelling reason for terrorism offences to involve a mandatory jury trial?

The *Criminal Code* contains a number of offences that at first reading seem to compel trial by judge and jury. These are found in section 469 and include murder, treason and crimes against humanity. Even with these offences, however, the accused and the Attorney General can consent under section 473(1) to a trial by a Superior Court judge. Thus, there are no offences in the *Criminal Code* that must always be tried by a jury. The recommendation made by AIFVA that no terrorism prosecutions be held before a judge alone would require creating a new and unprecedented category of offences that could not be tried by judge alone even if the Crown and defence were prepared to consent to trial by judge alone.

---

311 Testimony of Ralph Steinberg, vol. 93, December 11, 2007, pp. 12364-12365.
312 Testimony of Hon. Ruth Krindle, vol. 94, December 12, 2007, p. 12425.
313 Testimony of Kent Roach, vol. 95, December 13, 2007, p. 12558.
314 Testimony of Kent Roach, vol. 95, December 13, 2007, p.12570.
315 MacFarlane Paper on Terrorist Mega-Trials, p. 301.
316 *Canada (Justice) v. Khadr*, 2008 SCC 28, [2008] 2 S.C.R. 125.

Requiring mandatory jury trials for all terrorism prosecutions would add further inflexibility to the present system. It could result in jury trials when both the Crown and the accused agree that a jury trial is not appropriate or even possible. The result could be lengthy trials that would tax the endurance of juries. The result, even with an expanded 16-member jury panel, could be mistrials that prevent important cases from reaching a verdict.

A less drastic alternative would be to add terrorism offences to the short list of offences under section 469 of the *Criminal Code*. Trial by jury would be required unless the Crown consented under section 473(1) to trial by judge alone. It would take away the option, exercised by Mohammad Momin Khawaja, the first person charged with a terrorism offence under the *Anti-terrorism Act*, to select trial by judge alone.

There are good reasons why those accused of terrorism offences may want to elect trial by judge alone. The facts or allegations in a terrorism cases may be both shocking and very well-publicized. The trial may involve evidence, including that relating to the accused's motives, which could have a significant prejudicial effect on the jury. A powerful argument is needed to justify restricting the choice of the accused about mode of trial.

Some might suggest that a mandatory jury trial will produce a more just verdict than trial by judge alone. However, there is no evidence to show this to be the case, and a decision to impose a mandatory jury trial should not be based on mere speculation that it will produce a better result. In addition, greater efficiency can be achieved in cases involving trial by judge alone – for example, the ability to decide questions of law that arise during the trial without having to excuse the jurors.

Recommendation 35:

It is recommended that:

a) the *Criminal Code* be amended to allow the judge in a jury trial to empanel up to 16 jurors to hear the case if the judge considers it to be in the interests of justice;

b) if more than 12 jurors remain at the start of jury deliberations, the 12 jurors who will deliberate be chosen by ballot of all the jurors who have heard the case;

c) the minimum number of jurors required to deliberate remain at 10;

d) the idea of having terrorism trials heard by a panel of three judges be rejected because it offers no demonstrable benefit; and

e) the call for mandatory jury trials in terrorism cases be rejected in view of the difficulties of long trials with juries and the accused's present ability to opt for trial by judge alone.

9.5.5 Addressing the Needs of Victims

Unlike most criminal trials, where the number of victims is limited, the Air India tragedy profoundly affected the lives of direct family members and others close to the victims. Accommodating the important needs of so many individuals at the trial was challenging. In fact, Gaul described the efforts of the Air India Crown Victims and Witnesses Service in dealing with the families of the Air India victims as "Herculean":

> It was a joint venture with the federal government in the sense of financing of the project. They provided the financing. We provided the…human resources, and it was [an] integral, absolutely integral part of the prosecution team of having a professional staff to be able to deal with the victim issues…of them coming into Vancouver, how to handle them in the sense of logistically, but also emotionally.
>
> . . .
>
> I think it's important that the resources are made available and the right people so to speak; again, you have to have people skills.... [Y]ou can put up with some difficult personalities or challenging personalities for a month or so, but if we're talking years, you have to have somebody who knows their field but also has strong interpersonal skills to deal with the emotional aspects of this case and can lead the team of people working with that person….[317]

Unfortunately, future terrorism trials could again see many victims or family members of victims. In such cases, the only way to deal humanely with their needs and to make the resulting trial workable is to provide carefully designed, culturally sensitive, comprehensive and adequately funded victim services. The approach to witness services in the Air India trial, detailed earlier in this chapter, may serve as a very useful model.

9.6 Conclusion

In his report for the Commission, Bruce MacFarlane notes that "…[t]wenty-first century terrorist trials are exceptionally complex in nature, and there is a demonstrable need to ensure that they do not collapse under their own weight."[318] The Air India trial reached a verdict despite significant obstacles. These included: the extraordinary length of the trial; huge costs; massive amounts of material to disclose, including documents that brought national security considerations into play; numerous motions, witnesses and exhibits; scores of defence and Crown counsel; hundreds of family members of the victims; and a very significant public profile. Much could have happened to prevent the trial from reaching a verdict.

---

317 Testimony of Geoffrey Gaul, vol. 88, December 4, 2007, pp. 11414-11415.
318 MacFarlane Paper on Terrorist Mega-Trials, p. 297.

The experience of the Air India trial offered several lessons that can help future terrorism trials reach a verdict. This chapter has also explored several other measures that will lead to the same result. Collectively, these lessons and measures can be summarized as follows:

- putting in place a project management team;
- early selection of a trial judge who can exercise firm control over the pre-trial and trial processes;
- organizing and controlling the pre-trial process more effectively to minimize pre-trial delays, and making rulings on many pre-trial motions that will continue to bind the parties even if the prosecution is severed into smaller prosecutions or a mistrial is declared;
- allowing omnibus hearings of related motions from all related trials;
- putting into place a process for early and staged disclosure, relying heavily on electronic disclosure and the ability of defence counsel to inspect material that is of only marginal relevance to the case;
- ensuring that funding is available to retain experienced counsel, both defence and Crown, who can better serve the interests of their clients and help the trial move forward efficiently;
- developing a more effective procedure for trial judges to deal with applications under section 38 of the *Canada Evidence Act*; and
- providing comprehensive services for the families of victims.

Many of these measures will also reduce the burden on juries. The likelihood of reaching a verdict in a jury trial can be further enhanced by empanelling additional jurors. The present situation, where there are no alternate jurors and no more than two jurors can be discharged once a trial has started without causing a mistrial, is unacceptable. It is an invitation to having an important terrorism prosecution like the Air India trial fail to reach a verdict.

As noted at the outset, Canada has had very little experience with terrorism prosecutions. This relative good fortune should not become an excuse for failing to address the deficiencies in the justice system that may derail future prosecutions. The gravity of terrorist acts and the compelling public interest in bringing prosecutions for those acts to a final verdict demands that Canada's justice system prepare for the exceptional challenges of terrorism prosecutions. That is the very least that can be expected of governments in Canada. The federal government should be prepared to lead through the limited but vital amendments to the *Criminal Code* proposed in this chapter. It should also be willing to enter into cost-sharing agreements with the provinces in order to serve the national interest in fair and efficient terrorism prosecutions.

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

CHAPTER X: RECOMMENDATIONS

Recommendations from Chapter II: Coordinating the Intelligence/ Evidence Relationship

Recommendation 1:

The role of the National Security Advisor in the Privy Council Office should be enhanced. The National Security Advisor's new responsibilities should be as follows:

- to participate in setting strategic national security policies and priorities;
- to supervise and, where necessary, to coordinate national security activities, including all aspects of the distribution of intelligence to the RCMP and to other government agencies;
- to provide regular briefings to the Prime Minister and, as required, to other ministers;
- to resolve, with finality, disputes among the agencies responsible for national security;
- to provide oversight of the effectiveness of national security activities; and
- to carry out the government's national security policy in the public interest.

In carrying our these new duties, the National Security Advisor should be assisted by a Deputy and by a staff of secondees from agencies which have national security responsibilities, such as CSIS, the RCMP, the CBSA, and DFAIT. The National Security Advisor should continue to support relevant Cabinet committees and serve as Deputy Minister for the CSE, but these duties could, if necessary, be delegated to the Deputy National Security Advisor or to another official within the office of the NSA.

Measures to enhance the role of the NSA should not be delayed until the enactment of legislation on a new national security privilege.

Recommendations from Chapter III: Coordinating Terrorism Prosecutions

Recommendation 2:

The role of the National Security Advisor should be exercised in a manner that is sensitive to the principles of police and prosecutorial independence and discretion, while recognizing the limits of these principles in the prosecution of terrorism offences. The principle of police independence should continue to be qualified by the requirement that an Attorney General consent to the laying of charges for a terrorism offence.

The Attorney General of Canada should continue to be able to receive relevant information from Cabinet colleagues, including the Prime Minister and the National Security Advisor, about the possible national security and foreign policy implications of the exercise of prosecutorial discretion.

Recommendation 3:

Terrorism prosecutions at the federal level should be supervised and conducted by a Director of Terrorism Prosecutions appointed by the Attorney General of Canada.

Recommendation 4:

The office of the Director should be located within the department of the Attorney General of Canada and not within the Public Prosecution Service of Canada. The placement of the proposed Director of Terrorism Prosecutions in the Attorney General's department is necessary to ensure that terrorism prosecutions are conducted in an integrated manner, given the critical role of the Attorney General of Canada under the national security confidentiality provisions of section 38 of the *Canada Evidence Act*.

Recommendation 5:

The Director of Terrorism Prosecutions should also provide relevant legal advice to Integrated National Security Enforcement Teams and to the RCMP and CSIS with respect to their counterterrorism work to ensure continuity and consistency of legal advice and representation in terrorism investigations and prosecutions.

Recommendation 6:

The Director of Terrorism Prosecutions should preferably not provide legal representation to the Government of Canada in any civil litigation that might arise from an ongoing terrorism investigation or prosecution, in order to avoid any possible conflict of interest.

Recommendation 7:

A lead federal role in terrorism prosecutions should be maintained because of their national importance and the key role that the Attorney General of Canada will play in most terrorism prosecutions under section 38 of the *Canada Evidence Act*. The Attorney General of Canada should be prepared to exercise the right under the *Security Offences Act* to pre-empt or take over provincial terrorism prosecutions if the difficulties of coordinating provincial and federal prosecutorial decision-making appear to be sufficiently great or if a federal prosecution is in the public interest.

Recommendation 8:

Provincial Attorneys General should notify the Attorney General of Canada through the proposed federal Director of Terrorism Prosecutions of any potential prosecution that may involve a terrorist group or a terrorist activity, whether or not the offence is prosecuted as a terrorism offence. The National Security Advisor should also be notified.

Recommendations from Chapter IV: The Collection and Retention of Intelligence: Modernizing the *CSIS Act*

Recommendation 9:

In compliance with the 2008 Supreme Court of Canada decision in *Charkaoui*, CSIS should retain intelligence that has been properly gathered during an investigation of threats to national security under section 12 of the *CSIS Act*. CSIS should destroy such intelligence after 25 years or a period determined by Parliament, but only if the Director of CSIS certifies that it is no longer relevant.

Recommendation 10:

The *CSIS Act* should be amended to reflect the enhanced role proposed for the National Security Advisor and to provide for greater sharing of information with other agencies.

Section 19(2)(a) of the *CSIS Act* should be amended to require CSIS to report information that may be used in an investigation or prosecution of an offence either to the relevant policing or prosecutorial authorities or to the National Security Advisor.

If the National Security Advisor receives security threat information from CSIS, he or she should have the authority, at any time, to provide the information to the relevant policing or prosecutorial authorities or to other relevant officials with a view to minimizing the terrorist threat. The National Security Advisor should make decisions about whether intelligence should be disclosed only after considering the competing demands for disclosure and secrecy. In every case, the decision should be made in the public interest, which may differ from the immediate interests of the agencies involved.

Intelligence prepared to assist the National Security Advisor in his or her deliberations, and the deliberations themselves, should be protected by a new national security privilege. The privilege would be a class privilege similar to that protecting information submitted to assist with Cabinet deliberations.

Recommendation 11:

To the extent that it is practicable to do so, CSIS should conform to the requirements of the laws relating to evidence and disclosure when conducting its counterterrorism investigations in order to facilitate the use of intelligence in the criminal justice process.

Recommendation 12:

In terrorism prosecutions, special advocates, given powers similar to those permitted under the *Immigration and Refugee Protection* Act, should be allowed to represent the accused in challenging warrants issued under section 21 of the *CSIS Act* or under Part VI of the *Criminal Code*. The special advocates should have access to all relevant information, including unedited affidavits used to justify the warrants, but should be prohibited from disclosing this information to anyone without a court order. Both the judges reviewing the validity of warrants and the special advocates should be provided with facilities to protect information that, if disclosed, might harm national security.

Recommendations from Chapter V: The Disclosure and Production of Intelligence

Recommendation 13:

Federal prosecutorial guidelines should be amended to make it clear to those who prosecute terrorism cases that only material that is relevant to the case and of possible assistance to the accused should be disclosed. Material of limited relevance – in the sense that it is not clearly irrelevant – should, in appropriate cases, be made available for inspection by the defence at a secure location.

Recommendation 14:

There is no need for further legislation governing the production for a criminal prosecution of intelligence held by CSIS. The procedures available under section 38 of the *Canada Evidence Act* provide an appropriate and workable framework for the trial court to determine whether production of such intelligence is warranted.

Recommendations from Chapter VI: The Role of Privileges in Preventing the Disclosure of Intelligence

Recommendation 15:

The RCMP and CSIS should each establish procedures to govern promises of anonymity made to informers. Such procedures should be designed to serve the public interest and should not be focused solely on the mandate of the particular agency.

Recommendation 16:

Section 19 of the *CSIS Act* should be amended to provide that information about an individual which is exchanged by CSIS with a police force or with the NSA does not prejudice claiming informer privilege.

Recommendation 17:

CSIS should not be permitted to grant police informer privilege. CSIS informers should be protected by the common law "Wigmore privilege," which requires the court to balance the public interest in disclosure against the public interest in confidentiality. If the handling of a CSIS source is transferred to the RCMP, the source should be eligible to benefit from police informer privilege.

Recommendation 18:

The *Canada Evidence Act* should be amended to create a new national security privilege, patterned on the provision for Cabinet confidences under section 39 of the Act. This new class privilege should apply to documents prepared for the National Security Advisor and to the deliberations of the office of the National Security Advisor.

Recommendations from Chapter VII: Judicial Procedures to Obtain Non-Disclosure Orders in Individual Cases

Recommendation 19:

The present two-court approach to resolving claims of national security confidentiality under section 38 of the *Canada Evidence Act* should be abandoned for criminal cases. Section 38 should be amended to allow the trial court where terrorism charges are tried to make decisions about national security confidentiality. Section 38 should be amended to include the criminal trial court in the definition of "judge" for the purposes of dealing with a section 38 application that is made during a criminal prosecution.

Recommendation 20:

In terrorism prosecutions, there should be no interim appeals or reviews of section 37 or 38 disclosure matters. Appeals of rulings under sections 37 or 38 should not be permitted until after a verdict has been reached. Appeals should be heard by provincial courts of appeal in accordance with the appeal provisions contained in the *Criminal Code*. If not already in place, arrangements should be made to ensure adequate protection of secret information that provincial courts of appeal may receive. Sections 37.1, 38.08 and 38.09 of the *Canada Evidence Act* should be amended or repealed accordingly.

Recommendation 21:

Security-cleared special advocates should be permitted to protect the accused's interests during section 38 applications, in the same manner as they are used under the *Immigration and Refugee Protection Act*. Either the accused or the presiding judge should be permitted to request the appointment of a special advocate.

Recommendation 22:

The Attorney General of Canada, through the proposed Director of Terrorism Prosecutions, should exercise restraint and independent judgment when making claims under section 38 of the *Canada Evidence Act* and avoid using overly broad claims of secrecy.

Recommendation 23:

The Federal Prosecution Service Deskbook and other policy documents that provide guidance about making secrecy claims should be updated to encourage the making of requests to foreign agencies to lift caveats that they may have placed on the further disclosure of information. These documents should also be updated to reflect the evolution of national security confidentiality jurisprudence. In particular, the Deskbook should direct prosecutors to be

prepared to identify the anticipated harms that disclosure would cause, including harms to ongoing investigations, breaches of caveats, jeopardy to sources and the disclosure of secret methods of investigations. The Deskbook should discourage reliance solely on the "mosaic effect" as the basis for making a claim of national security confidentiality.

Recommendations from Chapter VIII: Managing the Consequences of Disclosure: Witness and Source Protection

Recommendation 24:

A new position, the National Security Witness Protection Coordinator, should be created. The Coordinator would decide witness protection issues in terrorism investigations and prosecutions and administer witness protection in national security matters. The creation of such a position would require amendments to the *Witness Protection Program Act*.

The National Security Witness Protection Coordinator should be independent of the police and prosecution. He or she should be a person who inspires public confidence and who has experience with criminal justice, national security and witness protection matters.

Where appropriate and feasible, the Coordinator should consult any of the the following on matters affecting witness and source protection: the RCMP, CSIS, the National Security Advisor, the proposed Director of Terrorism Prosecutors, Public Safety Canada, Immigration Canada, the Department of Foreign Affairs and International Trade and the Correctional Service of Canada. The Coordinator would generally work closely with CSIS and the RCMP to ensure a satisfactory transfer of sources between the two agencies.

The National Security Witness Protection Coordinator's mandate would include:

- assessing the risks to potential protectees resulting from disclosure and prosecutions, as well as making decisions about accepting an individual into the witness protection program and the level of protection required;

- working with relevant federal, provincial, private sector and international partners in providing the form of protection that best satisfies the particular needs and circumstances of protectees;

- ensuring consistency in the handling of sources and resolving disputes between agencies that may arise when negotiating or implementing protection agreements (this function would be performed in consultation with the National Security Advisor);

- providing confidential support, including psychological and legal advice, for protectees as they decide whether to sign protection agreements;
- negotiating protection agreements, including the award of payments;
- providing strategic direction and policy advice on protection matters, including the adequacy of programs involving international cooperation or minors;
- providing for independent and confidential arbitration of disputes that may arise between the protectee and the witness protection program;
- making decisions about ending a person's participation in the program;
- acting as a resource for CSIS, the RCMP, the National Security Advisor and other agencies about the appropriate treatment of sources in terrorism investigations and management of their expectations;
- acting as an advocate for witnesses and sources on policy matters that may affect them and defending the need for witness protection agreements in individual cases.

The National Security Witness Protection Coordinator would not be responsible for providing the actual physical protection. That function would remain with the RCMP or other public or private bodies that provide protection services and that agree to submit to confidential arbitration of disputes by the Coordinator.

Recommendations from Chapter IX: Managing the Consequences of Disclosure: The Air India Trial and the Management of Other Complex Terrorism Prosecutions

Recommendation 25:

To make terrorism prosecutions workable, the federal government should share the cost of major trials to ensure proper project management, victim services and adequate funding to attract experienced trial counsel who can make appropriate admissions of fact and exercise their other duties as officers of the court;

Recommendation 26:

The trial judge should be appointed as early as possible to manage the trial process, hear most pre-trial motions and make rulings; these rulings should not be subject to appeal before trial;

Recommendation 27:

The *Criminal Code* should be amended to ensure that pre-trial rulings by the trial judge continue to apply in the event that the prosecution subsequently ends in a mistrial or is severed into separate prosecutions. The only case in which rulings should not bind both the accused and the Crown should be if there is a demonstration of a material change in circumstances;

Recommendation 28:

The *Criminal Code* should be amended to allow omnibus hearings of common pre-trial motions in related but severed prosecutions. This will facilitate severing terrorism prosecutions that have common legal issues where separate trials would be fairer or more manageable. All accused in the related prosecutions should be represented at the omnibus hearing. Decisions made at omnibus hearings should bind the Crown and accused in subsequent trials unless a material change in circumstances can be demonstrated. Such rulings should be subject to appeal only after a verdict.

Recommendation 29:

Electronic and staged disclosure should be used in terrorism prosecutions in order to make them more manageable. Disclosure should occur as follows:

Recommendation 30:

The Crown should be permitted to provide in electronic form any material on which it intends to rely and should have the discretion to provide paper copies of such material. If the Crown decides to use electronic disclosure, it must ensure that the defence has the necessary technical resources to use the resulting electronic database, including the appropriate software to allow annotation and searching;

Recommendation 31:

Material on which the Crown does not intend to rely but which is relevant should be produced in electronic format, and the necessary technical resources should be provided to allow the use of the resulting electronic database;

Recommendation 32:

The Crown should be able to disclose all other material that must be disclosed pursuant to *Stinchcombe* and *Charkaoui* by making it available to counsel for the accused for manual inspection. In cases where the disclosure involves sensitive material, the Crown should be able to require counsel for the accused to inspect the documents at a secure location with adequate provisions for maintaining the confidentiality of the lawyer's work. Defence counsel should have a right to copy information but subject to complying with conditions to safeguard the information and to ensure that it is not used for improper purposes not connected with the trial;

Recommendation 33:

The trial judge should have the discretion to order full or partial paper disclosure where the interests of justice require; and

Recommendation 34:

The authority and procedures for electronic disclosure should be set out in the *Criminal Code* in order to prevent disputes about electronic disclosure.

Recommendation 35:

It is recommended that:

a) the *Criminal Code* be amended to allow the judge in a jury trial to empanel up to 16 jurors to hear the case if the judge considers it to be in the interests of justice;

b) if more than 12 jurors remain at the start of jury deliberations, the 12 jurors who will deliberate be chosen by ballot of all the jurors who have heard the case;

c) the minimum number of jurors required to deliberate remain at 10;

d) the idea of having terrorism trials heard by a panel of three judges be rejected because it offers no demonstrable benefit; and

e) the call for mandatory jury trials in terrorism cases be rejected in view of the difficulties of long trials with juries and the accused's present ability to opt for trial by judge alone.