VOLUME ONE
THE OVERVIEW

CHAPTER IV: INTELLIGENCE AND EVIDENCE

4.0 Introduction

Terrorism is both a serious security threat and a serious crime. Secret intelligence collected by Canadian and foreign intelligence agencies can warn the Government about terrorist threats and help prevent terrorist acts. Intelligence can also serve as evidence for prosecuting terrorism offences.

Volume Three addresses the issues that arise from using intelligence as evidence in criminal investigations and trials. Using intelligence as evidence can create a tension between the secrecy essential for the operations of the intelligence community and the openness demanded by the criminal trial process. Volume Three recommends having the National Security Advisor resolve this tension, acting in the public interest instead of in the sometimes narrower interests of the agencies involved.

The delicate balance between openness and secrecy presents challenges at each stage of the response to the threat of terrorism. Each terrorist threat is unique, and will require a response tailored to the specific circumstances of the threat, so it follows that there can be no presumptively "best" response. In some cases, it will clearly be appropriate to engage the police early on. In others, it may better serve the public interest to allow intelligence agencies to continue to monitor and report on the threat or to use other, non-police, agencies to disrupt an evolving plot. The most effective use of intelligence may not even involve the criminal justice system.

Canadian efforts against terrorism involve many entities, including the Canadian Security Intelligence Service (CSIS), the Canada Revenue Agency (CRA), 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 has its own mandate and rules governing how it carries out that mandate. The mandates sometimes overlap.

4.1 Secrecy vs. Openness

Even with the best intentions, coordination and effective communication among the many agencies involved in the counterterrorism effort in Canada can be very difficult.

Both the pre-bombing and post-bombing phases of the Air India tragedy demonstrate the challenges that these agencies experienced in communicating effectively with each other and in respecting each others' rules and requirements while, at the same time, looking out for their own institutional interests.

During the pre-bombing phase, CSIS did not get important information from other agencies, including CSE and the RCMP, and hence was unable to provide a meaningful assessment of the threat to Air India flights. In the post-bombing phase, CSIS collected and dispersed information according to its own rules and intelligence requirements, but in the process made the information unavailable to or unusable by the criminal justice system. This impaired the quality of the evidence available to the prosecution and compromised the fair trial rights of the accused. When CSIS passed information to the RCMP, the RCMP was often careless in respecting caveats or in appropriately protecting sources and methods. As for the criminal justice system, its focus on complete and wide-ranging disclosure repeatedly encountered resistance in the form of the intelligence community's basic imperative to protect the confidentiality of its sources, methods and information.

While CSIS faces potentially adverse consequences as a result of sharing information with the police, there are no similar consequences for other agencies that share information with CSIS. There is no excuse for any agency failing to share information with CSIS. Security-related threat information collected by the RCMP for law enforcement purposes can, and ought to be, shared with CSIS in all but the rarest of circumstances. The Commission does not view the report or recommendations of the O'Connor Commission as being in any way inconsistent with this observation.

Agencies must share information with each other to respond effectively to terrorist threats. However, Canadian agencies have developed a culture of managing information in a manner designed to protect their individual institutional interests. This approach compromises coordination and effective communication among agencies.

The decision of an intelligence agency to share intelligence with the police may have far-reaching implications for ongoing intelligence investigations, for the agency's sources and for the targets of investigations. The governing imperative for intelligence-gathering agencies is to preserve tight restrictions on the dissemination of information. This imperative makes sense, for several reasons. First, collecting intelligence is largely a clandestine activity. Foreign governments and intelligence services restrict, often explicitly, the further disclosure of their intelligence as a condition of sharing it with CSIS. Valuable intelligence often comes from sources who cannot be revealed publicly without jeopardizing their continuing usefulness and, possibly, their safety. Almost always, intelligence agencies prohibit the dissemination of information beyond CSIS, seriously impeding law enforcement. This is a reality of the modern security intelligence environment.

Second, intelligence agencies resist public disclosure of information due to the realistic fear of compromising the investigation for which it has been collected. Public disclosure, or even limited disclosure to law enforcement, can interfere with sensitive intelligence investigations and even lead to their termination. Compromised investigations may harm Canada's international strategic interests and threaten the safety of individuals involved in gathering intelligence.

A further plausible reason for CSIS resisting disclosure is rooted in the intrusive means by which it is authorized to collect intelligence. 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 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. Easy disclosure to the police of material collected under a CSIS warrant could risk, in the words of Geoffrey O'Brian, one of the first civilian employees of CSIS, turning CSIS into a "cheap cop shop."

These reasons explain and, in some measure, justify resistance by CSIS to public disclosure of intelligence. However, there are situations in which the disclosure of intelligence by CSIS to law enforcement is in the public interest.

From the point of view of the criminal justice system, the ruling imperative is the public production of as much potentially relevant information as possible. The right to a fair trial, entrenched in section 7 of the *Charter*, requires that all relevant information in the possession of the prosecution be given to the accused person, no matter whether it tends to support or to undermine the case for the prosecution. In our open system of justice, the information upon which guilt or innocence is determined must be made public. To justify the serious sanctions that can be imposed by the criminal justice system, the system requires reliable proof to a very high standard. These requirements cannot be circumvented or compromised. As a result, the compelling reasons for the intelligence community to maintain secrecy are balanced by equally compelling reasons for the criminal justice system to require openness. Effective protection of national security depends on both the intelligence-gathering system and the criminal justice system. Effective cooperation among agencies in sharing and using intelligence is not merely a subject of theoretical debate; it is a practical necessity.

4.2 Concurrent National Security Mandates and Information Sharing

The counterterrorism mandates of CSIS and the RCMP overlap to a significant degree. The consequences of a terrorist threat fall squarely within the core mandate of CSIS, which is to advise the Government of Canada on the nature and extent of threats to national security. As a criminal offence, terrorism is equally central to the RCMP mandate to investigate and prosecute serious crimes. The extent of the overlap is highlighted by the 2001 *Anti-terrorism Act* definition of the criminal offence of "terrorism." Terrorism extends both to completed acts of violence and to the planning and providing of assistance for such acts, whether or not they have come to fruition. CSIS and the RCMP are each legitimately involved in investigating the same activities.

Developments in criminal jurisprudence have put pressure on CSIS to make intelligence public in the criminal process. The Supreme Court of Canada decision in *R v. Stinchcombe* clarified beyond all debate that the prosecution has an obligation to disclose all potentially relevant material in its possession to the accused. At around the same time as the *Stinchcombe* decision, courts began looking behind claims of "national security confidentiality," testing the accuracy of the affidavits used to justify search warrants and wiretap applications, before admitting material gathered on the basis of such warrants into evidence at trial. These developments set the CSIS imperative of secrecy directly into conflict with the criminal justice system's requirement to disclose all potentially relevant information to the defence.

Because CSIS will usually begin the investigation of a threat well before there is any element of criminality, it will have much more information than will the RCMP. Once engaged in the investigation, however, the RCMP will want as much information from CSIS as it can get. CSIS information might be vital in that it may help the RCMP to understand the threat and to fill in any gaps in the body of information in its case.

For reasons already discussed, CSIS may be cautious about disclosing – and may even be categorically unwilling to disclose – information to the RCMP without a guarantee that the information will not be made public. Understandably, the RCMP cannot make such an assurance. If its own investigation leads to a prosecution, the RCMP will be required to disclose all potentially relevant information to the Crown and, eventually, that information will be disclosed to the defence and perhaps made public in court. Because of this, CSIS might try to avoid providing the information to the RCMP to protect the viability of its ongoing investigation.

These opposing interests over the use of CSIS intelligence can, in the extreme, lead to the unpalatable choice known as "disclose or dismiss": either disclose relevant information to the defence, even if it may contain sensitive intelligence, or protect the information, but risk failure to proceed with a case against an accused terrorist.

The "disclose or dismiss" dilemma has arisen in terrorism prosecutions both before and after *Stinchcombe*. This has resulted in the termination of several prosecutions before verdicts were reached. Notably, two of these have involved allegations of Sikh extremism. In one of the two, Talwinder Singh Parmar was the accused.

Paradoxically, the risk to criminal cases presented by the desire to protect sensitive intelligence has motivated the RCMP to avoid acquiring information from CSIS.

As discussed in detail in Volume Three, there are numerous ways to avoid the conflict between the desire to keep intelligence secret and the obligation to disclose potentially relevant information in a criminal trial. However, the perception that a choice may have to be made results in both CSIS and the police looking for ways to keep the intelligence out of the hands of the police. No matter how unintentional, the result will be to impoverish the response to terrorist threats. Something has to change in the approach taken towards the transfer of intelligence to the hands of law enforcement.

4.3 Ineffective Responses to the Disclosure Dilemma

4.3.1 Informal Solutions

The evidence shows that both CSIS and the RCMP, though they both may regard the result as far from optimal, have concluded that the best management of the potential "disclose or dismiss" dilemma is to avoid the problem entirely by ensuring that the minimum of potentially disclosable intelligence is passed from CSIS to the RCMP.

This misguided strategy is not new to either agency. From its inception, the "civilianization" of CSIS led it to adopt the mantra that "CSIS does not collect evidence." CSIS policies had the effect of rendering most CSIS information unusable in court and of limited value to the police. There may have been no nefarious purpose behind these policies. They accorded with the overwhelming sentiment at that time that a clean line needed to be drawn between CSIS as a civilian intelligence service and the RCMP as a law enforcement agency.

The consequences of the erasure of the Parmar tapes demonstrated that the policies regarding the collection and storage of information adhered to in order to protect CSIS information from disclosure in court did not in fact make CSIS intelligence irrelevant or immune from disclosure. The information on the destroyed tapes might have been of no use to either the prosecution or the defence in the Air India trial, and it might have been inadmissible at the trial based on a number of principles under the law of evidence. Still, the destruction of the tapes prevented the prosecution from disclosing their contents to the accused. This led to the worst possible results for CSIS and for the prosecution. The tapes were ruled disclosable and their destruction was held to be an abuse of process.

The larger lesson from this episode, one that may not be fully understood as yet by CSIS or the RCMP, is that efforts to keep potentially relevant CSIS information out of the hands of the RCMP are not effective. Disclosure obligations are engaged by the potential relevance of the information, not by its evidentiary status or by who holds it. It is for this reason that the philosophy of "the less information we receive from CSIS, the better" (curiously described in testimony as a "less is more" philosophy), adopted by the RCMP, is equally unlikely to shield CSIS intelligence from disclosure or to protect prosecutions in which the information is not disclosed.

The philosophy of "the less information we receive from CSIS, the better" is based on an assumption that the obligation to disclose would apply only to material that is in the hands of the RCMP; if CSIS did not provide material to the RCMP, the material would be deemed not to be in the Crown's possession and there would be no obligation to disclose that material to the defence.

The fact is that relevance, not custody, determines what the prosecution must disclose to the defence. There may be a privilege or legally recognized right that a person or institution may raise to persuade a court that, despite relevance, the material ought not to be disclosed. However, it is not possible to avoid the obligation to disclose simply by withholding the information from the police in the first place. Accordingly, the prosecution should pursue all relevant material, particularly if the information is in the hands of government entities that have investigated the matter now before the trial court.

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" should be abandoned. A better approach, whenever possible, is for CSIS to collect intelligence in counterterrorism investigations with the expectation that it may be disclosed or used as evidence in court.

4.3.2 Proposed Legislative Changes

From time to time, both CSIS and the RCMP have proposed that information-sharing challenges might be resolved through legislation. In general terms, these proposals range from the removal of legislative barriers to the flow of information from CSIS to the RCMP to the creation of legislative limits on the information that the criminal justice system can demand from CSIS. Each of these proposals addresses only one aspect of the problem, and thus will ultimately be ineffective in serving the public interest.

The Attorney General of Canada (AGC) can apply to the Federal Court to prevent disclosure of sensitive national security information by invoking section 38 of the *Canada Evidence Act*. Where disclosure for purposes of criminal proceedings is involved, the Federal Court examines whether the material could cause harm

to Canada's national security or international relations. If the answer is "no," the Court will refuse to bar disclosure. If the answer is "yes," the Court will consider whether failure to disclose will harm the fair trial rights of the accused person. If the answer to this second question is "no," the Court will bar disclosure outright. If the answer is "yes," the Court will still bar disclosure, but can consider a range of possible remedies, including releasing edited documents or providing unclassified summaries of the documents or information in question in order to mitigate the effect of barring direct disclosure.

This process allows CSIS to protect sensitive intelligence information, but both CSIS and the RCMP see the process as having several significant drawbacks. The outcome is inherently uncertain. Neither CSIS nor the RCMP can know at the beginning of the process – the point of disclosure by CSIS to the RCMP – what its conclusion will be.

Furthermore, the process for determining whether sensitive intelligence information can be withheld does not end with the Federal Court's determination of the section 38 application, or even with the conclusion of any appeals to the Federal Court of Appeal and Supreme Court of Canada. Whatever the ruling by the Federal Court, the Attorney General of Canada still has jurisdiction to order disclosure or to prohibit disclosure of any information or document. All this clearly adds to the uncertainty for CSIS, and also introduces uncertainty for the RCMP and, ultimately, for the prosecution.

It is, therefore, not surprising that, at the extreme end of the spectrum, proposals have been put forth for a legislated privilege which would remove any national security material from the criminal justice system. Intelligence would not need to be disclosed to the accused in the same way that the identity of a police informer is not disclosed.

In a post-*Charter*, post-*Stinchcombe* world, it is not possible simply to ignore the right of an accused person to a fair trial, a right that includes disclosure of all relevant information capable of assisting an accused person in making "full answer and defence" to the charges. No blanket privilege can trump these *Charter* rights. Even the police informer privilege, perhaps as bullet-proof a privilege as can exist in the criminal law sphere, cannot prevail when "innocence is at stake."

To ensure that a "national security privilege" would comply with the *Charter*, it would be necessary to qualify the privilege by requiring disclosure to the extent necessary to ensure a fair trial. This would produce the same situation as when the trial judge considers whether any orders under section 38 infringe an accused person's right to a fair trial. The intelligence information might not need to be disclosed, but if it were not disclosed, the case against the accused might have to be dismissed.

A different proposal to limit the flow of information in the disclosure process involves the suggestion that the disclosure requirements set out in *Stinchcombe* should be limited by statute. This is a suggestion often made by the police,

who bear the brunt of the *Stinchcombe* disclosure requirements, which are sometimes described as the most onerous of any Western democracy. However, insofar as the problem of excessive resources devoted to needless disclosure applies to the criminal justice system in general, one should be cautious about identifying this problem as residing in the *Stinchcombe* test itself.

The constitutional dimension of *Stinchcombe* consists of a right to all relevant information touching on the accused's ability to defend him- or herself. In order to make such disclosure, someone must go through the raw material to identify all potentially relevant information and then identify that which is actually relevant. This will require separating the clearly irrelevant from the possibly relevant (which is another way of saying "not clearly irrelevant") and, then, the actually relevant from the possibly relevant.

However, this is not to say that practical and cost-saving measures in relation to *Stinchcombe* disclosure obligations cannot be taken. Volume Three proposes that, in terrorism prosecutions, 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. Material on which the Crown does not intend to rely, but which is relevant, should be produced in electronic format. The Crown should be able to disclose all other material that must be disclosed pursuant to *Stinchcombe* and the 2008 decision in *Charkaoui* by making it available to the accused for manual inspection.

In any event, whether the rules for initial disclosure obligations are broadly or narrowly articulated, the fundamental constitutional obligation is always the same: for a fair trial, the defence must have disclosure of all material necessary to make "full answer and defence."

On the other end of the spectrum are proposals designed to enhance the sharing of intelligence with police. Volume Three discusses an amendment to section 19(2) of the *CSIS Act* to remove the current CSIS discretion concerning whether or not to disclose information to police. However, solutions of this nature are paradoxically likely to do both less and more than one might expect.

On the one hand, requiring disclosure is not tantamount to ensuring that the information will be admissible at trial. There would still be an opportunity for CSIS to object to public disclosure at trial on national security grounds under section 38 of the *Canadian Evidence Act*, and thus potential "disclose or dismiss" situations would not be avoided.

On the other hand, mandatory disclosure would have the unsatisfactory result of giving the RCMP the power to decide unilaterally what should be done with sensitive CSIS information.

The problem is that allowing the needs of the criminal justice system to take priority over other considerations will not always be in the best interests of

Canada. There may be good reasons for CSIS to avoid passing information to the RCMP. Leaving the choice of whether and when to commence a criminal investigation to the RCMP is unlikely to lead to better decision-making.

Any workable legislative changes cannot be based upon an a *priori* view that favours one of either law enforcement or the intelligence community over the other. Instead of approaching these issues from the perspective of individual agency concerns, the solution lies in making changes that allow for the public interest to be identified and acted upon.

4.4 Towards the Effective Management of the "Intelligence into Evidence" Problem

No "silver bullet" can exempt relevant intelligence from disclosure without consequences for the viability of a criminal prosecution. Once the intelligence and law enforcement communities accept that reality, they can focus on realistic and pragmatic practices and procedures that can minimize the potential for adverse consequences caused by using intelligence in criminal prosecutions.
First and foremost, the goal of such an approach should be to establish means to avoid a stark choice between the needs of a fair trial and those of national security. A realistic and pragmatic approach by the intelligence community would be to recognize that, as long as the criminal justice system remains an important means by which Canada seeks to deal with terrorism, intelligence may be relevant to the criminal justice system from the moment a terrorist conspiracy begins to unfold.

For that reason, it is necessary for the intelligence community to abandon the notion that "CSIS does not collect evidence" as a justification for practices that compromise the use of CSIS information in ensuing criminal investigations or prosecutions. The duty of disclosure of relevant information is entirely separate and distinct from the issue of whether the means by which the information was gathered, preserved and stored make it admissible as evidence at trial. CSIS has nothing to lose by ensuring that its practices in gathering, retaining and sharing information do not compromise the potential admissibility of the information as evidence in a criminal trial.

So long as the information is relevant, it will have to be disclosed, subject to national security privilege. On the other hand, a failure to follow such procedures can profoundly and, in some cases, irremediably, harm the interests of the justice system by making it more difficult to combat terrorism. Failure to provide prosecutors with usable information can compromise the viability of terrorism prosecutions to the extent that the ability to provide a fair trial to accused persons may be impaired, as illustrated by Justice Josephson's ruling on the erasure of the Parmar tapes in the Malik and Bagri trial.

In response to the Supreme Court of Canada's 2008 decision in *Charkaoui*, CSIS may now be attempting to reform its internal procedures for the retention

of information to comply with the Court's observations about CSIS retention obligations. As it approaches this task, CSIS should adopt procedures and provide training that will ensure that the methods by which information is retained and stored are capable of serving the interests of both the intelligence and law enforcement communities. This should include procedures for retention of the original materials (documents, interview notes, audio or video recordings) as well as practices to ensure demonstrable continuity of possession. It would be useful for the Service to seek the advice of the RCMP and the Department of Justice on the best approach to this.

Self-restraint and self-discipline in and by the institutions involved in the intelligence community and the criminal justice system would serve them well in combatting this problem. It is time for each institution, and the actors within it, to adopt a broader perspective and to avoid patterns of behaviour that may serve narrow institutional interests well but the public interest poorly.

For the intelligence community, this means not overstating the need for secrecy. For defence counsel, it means avoiding burdening the court with frivolous pre-trial applications. For prosecutors, it means avoiding "overcharging." For judges, it means becoming less tolerant of tactics used by counsel to try, for partisan advantage, to bring national security interests into conflict with the right to a fair trial. These issues, as well as the sheer volume of disclosure, can make the trial process cumbersome and, seemingly, out of control.

Defence counsel should abandon frivolous pre-trial applications, which lengthen proceedings, making criminal trials a war of attrition. A mature attitude and increased cooperation among counsel are needed. Many pre-trial applications can be avoided by using agreed statements of facts. Much of the "bulk" of a criminal trial can also be reduced by agreed statements of fact and admissions of matters not in dispute, allowing the judge to focus on what is truly in dispute.

Prosecutors should lay charges only for acts that they can prove. Prosecutors should not lay every possible charge against as many accused as possible. These "loaded indictments" unduly complicate criminal proceedings and bog them down in lengthy procedural wrangling.

Trial judges bear a significant responsibility. They are ultimately in charge of their courtroom and of the trial process. Too often they are timid and unwilling to rein in wayward counsel. Trial judges must make greater efforts to keep trials on track and focused on relevant matters. They need to develop a relationship with counsel so that all appreciate the need to cooperate.

None of this is intended to diminish the adversarial process. Rather, it is meant to focus the criminal trial on what is truly at issue and requires a determination to do so, be it about alleged breaches of the *Charter* or about an essential element of a criminal charge.

Volume Three contains a detailed discussion of possible procedural changes that may better enable the criminal justice system to cope with the unique challenges of terrorism prosecutions. The Commission gave careful consideration to suggestions for changes, including those from the Air India Victims Families Association. The terms of reference required the Commission to examine whether there is merit in having terrorism cases heard by a three-judge panel. The panel could replace a judge sitting alone or a judge and jury. While the Commission understands the thinking behind considering this mode of trial, it has concluded that the resulting procedural and legal complexities would make three-judge panels impractical and inadvisable.

4.5 Reforming Decision-Making

Even with the best efforts of the institutions involved in national security and criminal justice issues, their competing interests in the "intelligence-evidence" debate cannot easily be reconciled. An effective means of resolving these conflicts is necessary.

At several key times, choices may need to be made between the legitimate interests of the intelligence community and those of the criminal justice system. For each of those times, effective resolution will depend on the continual improvement of the decision-making process rather than on any formula for weighing the importance or the legitimacy of the competing interests. Former Commissioner Zaccardelli astutely observed that such decisions need to be made "in the interests of Canada." To resolve differences between competing interests in a manner that places the broader public interest above the narrower concerns of any agencies involved, the decision-maker must be sufficiently independent of the conflicting agencies.

4.5.1 The National Security Advisor

The first major point at which the interests of the intelligence community may diverge from those of the criminal justice system occurs when CSIS decides whether it should disclose information to a police agency about a possible terrorism offence.

CSIS and the RCMP share the reasonable expectation that the criminal justice system will be a vital tool for responding to planned terrorist acts. The police will investigate such plans, the Crown will prosecute and the courts will adjudicate. Testimony heard by the Commission suggests that CSIS will usually have no objection to disclosing such information to the RCMP in most cases. As CSIS adopts procedures about the disclosure of the intelligence that it gathers for use in criminal proceedings, the percentage of cases in which CSIS voluntarily discloses intelligence to the RCMP will likely rise.

Nevertheless, the possibility of a police investigation and resulting criminal prosecution can mean that CSIS might lose control over the further disclosure of

its intelligence. In such an event, the identities of CSIS sources and employees, the secrets of its allies and the integrity of its long-term investigations may be jeopardized. For that reason, it seems inevitable that CSIS will sometimes be reluctant to pass intelligence to the police, or that it will decide to postpone such disclosure.

The *CSIS Act* gives CSIS discretion about whether and when to disclose intelligence to the police. It is neither reasonable nor efficient to put CSIS in the position of weighing its own interests against those of law enforcement and, possibly, expecting CSIS to decide against its own interests.

Disclosure decisions related to the implementation of the government's overall anti-terrorism strategy should be made by the National Security Advisor (NSA) to the Prime Minister. Because the NSA reports only to the Prime Minister, it is appropriate that the ultimate responsibility for deciding what Canada's national interest requires remain at the highest level of government. The NSA is intimately familiar with the needs and the interests of the intelligence community and, as a result, has a broad understanding of the overall national security landscape and the potential impact of the involvement of the criminal justice system.

The courts and the police must remain free from external direction. The police must be independent of government direction about when and what they investigate, for example. For this reason, NSA would not attempt to direct RCMP investigators. However, the NSA should decide if and when CSIS intelligence should be passed to the RCMP if CSIS initially is reluctant to do so. CSIS would then be required to pass the intelligence to the RCMP, which in turn would use the intelligence to decide whether a police investigation is warranted. The NSA would provide high level coordination of the anti-terrorism effort, while taking into account the interests of CSIS and the RCMP.

The NSA would require assistance in determining the possible effects of any of its decisions on CSIS, the police and on the criminal justice system. The NSA would need support in assessing the usefulness of passing the information to law enforcement agencies. The NSA should have secondees from the RCMP on staff. These secondees would be able to inform the NSA regarding which investigations the police are likely to pursue. 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.

The NSA should be someone who understands intelligence issues and who acts independently in helping to arbitrate differences of opinion between government agencies. It is not necessary that the NSA be recruited within government. A premium should be placed on finding an individual with sufficient stature and experience to command the respect of the intelligence community, while also having the Prime Minister's confidence.

4.5.2 Director of Terrorism Prosecutions

The Attorney General of Canada has delegated most decisions about laying or staying charges and about the general conduct of prosecutions by federal prosecutors to the Public Prosecution Service of Canada. The bulk of federal prosecutions occur largely in specialized areas of criminal and quasi-criminal proceedings, including drug offences, *Competition Act* violations and immigration matters. However, this is not the appropriate institution to conduct terrorism prosecutions.

Terrorism is an existential threat to Canadian society in a way that murder, assault, robbery and other crimes are not. Terrorists reject and challenge the very foundations of Canadian society.

In any criminal matter, prosecutors examine several factors when deciding whether to prosecute. These factors always include the public interest. In terrorism cases, however, determining the best course of action consistent with the public interest involves different considerations from those in most criminal cases. In terrorism cases, the public interest is the aggregate of considerations which includes national security, international relations and the impact of prosecutions on sensitive intelligence operations.

For this reason, decisions about proceeding with a terrorism prosecution should be made by the Attorney General of Canada. The AGC has the resources and the legitimacy to take into account the public interest in a way that a delegate does not. A quasi arm's-length agency like PPSC is, by design, independent from government and, as such, is unsuited to make determinations about the public interest where terrorism cases are involved.

There is also a need for expertise in terrorism prosecutions. It would be advisable to create a position of Director of Terrorism Prosecutions (DTP), 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 of the *Canada Evidence Act* and give legal advice to agencies that collect intelligence and evidence in terrorism investigations.

The DTP should also be the decision-maker regarding the use of human intelligence sources as witnesses, as well as the liaison with police, intelligence services and foreign partners on matters concerning terrorism and national security.

The DTP should prosecute the criminal allegation and litigate all privilege claims, including those involving national security privilege. The DTP would work closely with the intelligence and law enforcement communities. This harmonized approach should promote carefully considered and fair terrorism prosecutions.

4.6 Determining National Security Privilege Claims

In a terrorism prosecution, the Attorney General of Canada may have to consider asking the Federal Court not to authorize the disclosure of information, in order to prevent harm to international relations, national defence or national security. If the Court agrees and refuses to authorize disclosure, the defence will be denied the information, but the prosecution will also be unable to rely on that information to secure a conviction. The legal basis for such a claim is found in section 38 of the *Canada Evidence Act*, and is known as national security privilege.

Two questions are central to the processes of litigating the section 38 claim and proceeding with the criminal trial. Would disclosure of the information harm Canada's interests? Is the disclosure of the information truly necessary for the defence to be able to respond to the charges?

The section 38 procedure requires two different courts to decide similar and closely related issues. Any non- 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 order, but also requires the trial judge to determine if any additional 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.

There are serious and irremediable disadvantages to the current two-court system for resolving issues of national security confidentiality. The Federal Court is in the difficult position of having to assess what the defence needs for full answer and defence in the absence of any intimate familiarity with the issues in the criminal trial. The trial judge, on the other hand, is given the impossible task of assessing the importance of the undisclosed information to the defence –without any direct access to that information.

The Federal Court does not have full information about the trial, while the trial judge does not have full information about the secret information that is subject to a non-disclosure order. Section 38 litigation, as it currently occurs, 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 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.

These problems are compounded by the delays to the criminal trial occasioned by the separate section 38 proceedings, and the possibility of appeals of section 38 issues to the Federal Court of Appeal and the Supreme Court of Canada. These interlocutory appeals can bring the criminal trial to a halt until they are resolved and may result in a mistrial because of unreasonable delay. Instead, there should be one decision-maker with access to all the relevant information and with the jurisdiction to make all the necessary findings and decisions. The current process in Canada, unique among Western democracies, needs to be changed.

Section 38 of the *Canada Evidence Act* should be amended so that claims of national security privilege in a trial of terrorism offences would be adjudicated by the trial judge as part of the criminal proceedings. Superior courts have constitutional jurisdiction to try criminal cases. Given the desirability of a single court, the most practical solution is to give the trial court jurisdiction over all aspects of disclosure and all claims of privilege. Appeals of decisions on section 38 claims should be allowed only after the verdict in the criminal trial.

The current procedure for dealing with section 38 claims does not allow the accused to participate, even though the decision about the claim may limit the disclosure of material that might help the accused's defence. The *Canada Evidence Act* should be amended to allow security-cleared "special advocates" to represent the interests of the accused, see the material for which the Attorney General of Canada is claiming national security privilege and, if warranted, challenge the claim. This role would be similar to that played by special advocates in immigration security certificate cases. Though passing information to clients would be prohibited, such special advocates would provide a much needed adversarial challenge to claims of national security privilege.

Special advocates would help to satisfy the constitutional right of an accused person to make full answer and defence. The accused would not be permitted to attend the hearing at which the privilege claim is determined or be informed about the information at contest unless the judge authorizes disclosure.

4.7 "Disclose or Dismiss": The Role of the Attorney General of Canada

At present, the Federal Court may, under section 38 of the *Canada Evidence Act*, order information to be disclosed despite a national security privilege claim by the Attorney General of Canada (AGC). However, the AGC can issue a certificate preventing disclosure that has been ordered. Besides the authority to override court orders, the AGC has powers relating to terrorism prosecutions. No terrorism charge can proceed without the Attorney General of Canada's consent.

The consequences of making these decisions are serious. The public interest should be the guiding factor in each case. Because the Attorney General of Canada already has the first and last word regarding terrorism criminal charges,

it stands to reason that the AGC should also be the ultimate decision-maker whenever the dilemma to disclose or dismiss arises.

Each of these powers of the Attorney General of Canada has stirred some controversy among critics who worry that the AGC's intervention can inject "politics" into what should be an "independent" judicial system. These criticisms do not stand up to scrutiny, because decisions made by the AGC are not based on partisan considerations. They can only be considered "political" in the broader sense that citizens in a democracy entrust their elected officials with the power to make decisions about the public interest in matters of national security.

Elected officials ultimately are responsible, with the Cabinet and the Prime Minister at the apex of that structure, to provide for the security of the nation. In addition to domestic consequences, national security decisions can have international ramifications, and therefore should not be made solely by the judiciary. The Attorney General of Canada, as Chief Law Officer of the Crown, is the appropriate official to bring both political authority and legal probity to decisions regarding terrorism criminal prosecutions that have an impact on the public interest.

In our legal and constitutional framework the ultimate decision-maker is the Attorney General of Canada. Where the decision truly is "disclose or dismiss," the current framework gets it right.

4.8 Source and Witness Protection

Law enforcement and intelligence agencies acknowledge that persons who provide information to them often do so at great risk to themselves and possibly to others close to them. Maintaining access to information from human sources may require the government to provide protection. Where individuals assisting the police are protected by police informer privilege, their identities are kept secret. If they do testify as witnesses, or if their identity is revealed inadvertently to their adversaries, these individuals can be protected through formal witness protection programs. In contrast, individuals who serve as sources to CSIS but who do not become witnesses do not have access to witness protection.

The Air India narrative demonstrates that, particularly when dealing with members of communities that may be preyed upon by extremists, individuals may often be willing to provide information to the authorities only if they are not required to expose their identities – by, for instance, testifying in a terrorism prosecution. The reluctance of sources to become witnesses is an important example of the problems caused by the traditional relationship between intelligence and evidence.

In terrorism cases, the current federal Witness Protection Program does not sufficiently address the multiple needs of witnesses and their families. The Commission recommends the creation of a position of "National Security

Witness Protection Coordinator" to deal with witness protection issues in terrorism matters.

One important responsibility of the Coordinator would be to determine who is allowed to enter the Witness Protection Program. The Coordinator could decide whether to offer protection to human sources and witnesses, and to their families, in criminal and intelligence investigations.

At present, the RCMP controls admission to the Program. Having the Coordinator make admission decisions would insulate decisions about protection of witnesses from decisions about investigations and prosecutions. It is not appropriate that a police agency with an interest in ensuring that sources agree to become witnesses make decisions about admission into a witness protection program. This is conflict of interest.

It is not clear whether police informer privilege extends to CSIS sources or, if it does not, whether it should. CSIS counterterrorism investigations are preventive. They often occur 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. Allowing CSIS to promise anonymity and to bring the privilege into play at that point might jeopardize subsequent terrorism prosecutions because those sources would not be able to testify. CSIS would perhaps be tempted to offer anonymity to assist it to collect intelligence, and much less interested in helping to make sources available to testify in terrorism prosecutions. This might lead to the privilege coming into play in particular situations in a way that serves the interests of CSIS, but not the broader public interest.

CSIS sources should nonetheless receive some protection against disclosure of their identities. The common law recognizes a category of privilege – the "Wigmore privilege" – that protects the confidentiality of information that is given in the expectation that it will be kept confidential, in circumstances when it is in the public interest to foster the type of relationship in which the confidential information was disclosed. At trial, the Wigmore privilege is typically invoked by the prosecution. However, the source may seek its protection if the prosecution does not.

Police informer privilege cannot be waived, except with the agreement of both the police and the informer. The informer alone can waive the Wigmore privilege, even if the party promising confidentiality (for instance, CSIS) does not agree.

4.9 Conclusion

Intelligence and law enforcement agencies both have legitimate, but sometimes competing, claims about how to use intelligence. Intelligence agencies may want to maintain the secrecy of the intelligence for operational reasons, while police agencies may want to see it made public as evidence in criminal prosecutions.

Neither claim trumps the other. The result is a tension between the two uses of intelligence. This is the "intelligence into evidence" conundrum.

Both types of agencies must re-examine their practices and procedures and find ways to avoid this dilemma. However, in some cases, a conflict will remain. The key is to ensure that, where a conflict remains about the possible disclosure of intelligence for a criminal prosecution, a single, independent decision-maker can resolve the conflict in the public interest. This decision-maker should have the experience, perspective and authority to transcend the narrower interests of the agencies involved. The recommendations in Volume Three are directed to changes in legislation, policy and procedure to assist in identifying and acting on this broader public interest.