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.