Although the accused can, in certain circumstances, be required to waive s.11 (b) to undertake some proceedings, and judges take a holistic and contextual approach to issues of trial delay, the accused, at the end of the day, has an enforceable right against trial delay. The spectre of a s.11 (b) violation adds constitutional force to the overall principle that terrorism prosecutions should be conducted efficiently for the good of both the accused and the public.

E) Summary

The demands for an efficient, yet fair and public, process for terrorism prosecutions all speak to the ability of Canada to use the criminal law to prosecute terrorism. The challenge is to ensure a process that provides an opportunity for the state to protect legitimate secrets while at the same time treating the accused fairly, respecting as much as possible the principle of open courts and resolving disputes about the reconciliation of these competing principles in an efficient and timely manner. A failure to resolve these difficulties will make it very difficult to bring terrorism prosecutions to verdict. A failure to prosecute terrorists and punish those whose guilt has been established beyond a reasonable doubt in a fair trial will erode public confidence in the administration of justice. It may also place Canada in breach of international obligations that require it to treat acts of terrorist violence as serious criminal offences.

III. The Use of Intelligence as Evidence

At times, intelligence may constitute some of the best evidence in terrorism prosecutions. Although security intelligence agencies target those who present a risk of involvement in terrorism, such targets may unexpectedly commit crimes, including many of the new terrorist crimes created in 2001. There are several barriers to using intelligence as evidence in terrorism prosecutions. One barrier is that security intelligence agencies generally are subject to less demanding standards when they collect information than the police. The rationale for such an approach is that security intelligence is designed to provide governments with secret information to help prevent security threats while the police collect evidence that can be used in public trials. Another barrier to using intelligence as evidence is that security intelligence agencies may have to disclose information surrounding the collection of intelligence as the price of using intelligence as evidence

This section of the study will start with an examination of whether material obtained through a CSIS wiretap could be admitted as evidence in a criminal trial. This raises the question of whether the CSIS wiretap scheme is consistent with the right against unreasonable search and seizure in s.8 of the Charter; whether it can justified as a reasonable limit under s.1 of the Charter; or whether unconstitutionally obtained CSIS wiretap evidence would be admitted or excluded under s.24(2) of the Charter. The leading case remains the *R. v. Atwal* terrorism prosecution in 1987, and this case will be discussed both as a precedent and a detailed case study.

The use of CSIS wiretaps will be examined in comparison with Criminal Code wiretap warrants. The 2001 ATA has made it easier in several respects to obtain Criminal Code wiretap warrants in terrorism investigations. As in the last section, it is important to revisit conventional wisdom about the relation between evidence and intelligence in light of changed legal and social circumstances as they affect terrorism investigations conducted by both the police and security intelligence agencies. One challenge with both CSIS and Criminal Code wiretaps is that the accused may gain access to confidential affidavits presented by the state to a judge to obtain the warrant. A case study of the Parmar prosecution in Hamilton will reveal how disclosure of material that would have identified a confidential informant caused that terrorism prosecution to collapse. Additional topics to be examined in this section will be the possible role that security cleared special advocates could play in challenges to Criminal Code and CSIS warrants, the collection and retention of intelligence under s.12 of the *CSIS Act*, the use of CSIS material under business records exceptions and the admissibility of various forms of intelligence collected outside Canada as evidence.

A) A Comparison Between CSIS Act and Criminal Code Electronic Surveillance Warrants

Electronic surveillance may, along with the recruitment of human sources, play a critical role in the investigation and prevention of terrorism. Section 21 of the *CSIS Act* allows a judge of the Federal Court to authorize the interception of communications or the obtaining of information on reasonable grounds that a warrant "is required to enable the Service to investigate a threat to the security of Canada" or to perform its duties to collect information about foreign states or persons under section 16 of

the Act.[166] This is a reasonable grounds standard, albeit one related to the investigation of a threat to the security of Canada and not necessarily a crime. It is not a standard based on mere suspicion.[167]

Section 186(1)(a) of the Criminal Code simply refers to the requirement that an authorization for electronic surveillance be in the "best interests of the administration of justice". This phrase has long been interpreted by the Supreme Court as requiring the judge to be satisfied that there are reasonable and probable grounds to believe that an offence has been or is being committed and that the intercept will provide evidence of that offence. In *Duarte*, the Supreme Court held that such a standard:

> ….meets the high standard of the *Charter* which guarantees the right to be secure against unreasonable search and seizure by subjecting the power of the state to record our private communications to external restraint and requiring it to be justified by application of an objective criterion. The reason this represents an acceptable balance is that the imposition of an external and objective criterion affords a measure of protection to any citizen whose private communications have been intercepted. It becomes possible for the individual to call the state to account if he can establish that a given interception was not authorized in accordance with the requisite standard.[168]

CSIS warrants are tied to that agency's mandate to investigate threats to the security of Canada while Criminal Code warrants are based on reasonable and probable grounds that a crime has been committed and that electronic surveillance will reveal evidence of the crime. Stated in the abstract, the differences between Criminal Code and CSIS warrants are great. As will be seen, however, some post 9/11 developments suggest that some of these differences may be diminishing.

---

166 *CSIS Act* s.21(1)

167 Section 12 of the CSIS Act contemplates a lower standard for investigation of "activities that may on reasonable grounds be suspected of constituting threats to the security of Canada". This section is discussed infra.

168 [1990] 1 S.C.R. 30. See also *R. v. Garofoli* [1990] 2 S.C.R. 1421.

B) The Constitutionality of Warrants Issued Under Section 21 of the CSIS Act

1. Section 8 of the Charter

In 1987, the Federal Court of Appeal considered the constitutionality of s.21 of the *CSIS Act*. The challenge arose in a terrorist prosecution as the accused sought to challenge the admissibility of a CSIS wiretap and the grounds for issuing the warrant. Mahoney J. for the majority of the Court of Appeal rejected the accused's argument that the warrant was invalid on its face because it did not relate the search to a specific offence and evidence of that offence. He concluded:

> The warrant in issue was granted in respect of a threat to national security, not the commission of an offence in the conventional sense. To conclude, as *Hunter et al. v. Southam Inc.* anticipated, that a different standard should apply where national security is involved is not necessarily to apply a lower standard but rather one which takes account of reality.
>
> Since the Act does not authorize the issuance of warrants to investigate offences in the ordinary criminal context, nor to obtain evidence of such offences, it is entirely to be expected that s. 21 does not require the issuing judge to be satisfied that an offence has been committed and that evidence thereof will be found in execution of the warrant. What the Act does authorize is the investigation of threats to the security of Canada and, inter alia, the collection of information respecting activities that may, on reasonable grounds, be suspected of constituting such threats. Having regard to the definition of "judge", s. 21(2)(a) of the Act fully satisfies, mutatis mutandis, the prescription of *Hunter et al. v. Southam Inc.* as to the minimum criteria demanded by s. 8 of legislation authorizing a search and seizure. [169]

Hugessen J.A. dissented and found a violation of the s.8 of the Charter because s.21 of the *CSIS Act*:

---

169 *Atwal v. Canada* (1987) 36 C.C.C.(3d) 161 at 183 (Fed.C.A.).

> …does not provide any reasonable standard by which the judge may test the need for the warrant. There is no requirement to show that the intrusion into the citizen's privacy will afford evidence of the alleged threat or will help to confirm its existence or non-existence. Nothing in the language of the statute requires a direct relationship between the information it is hoped to obtain from the intercepted communication and the alleged threat to the security of Canada. On the contrary, the relationship that is required to be established on reasonable grounds appears to be between the interception and the investigation of the threat. In practical terms this means that the statutory language is broad enough to authorize the interception, in the most intrusive possible manner, of the private communications of an intended victim of a terrorist attack without his knowledge or consent. Even more alarming, it would also allow an interception whose purpose was not directly to obtain information about the threat being investigated at all, but rather to advance the investigation by obtaining other information which could then be used as a bargaining tool in the pursuit of the investigation.[170]

The majority of the Court of Appeal stressed that *Hunter v. Southam* standards were not appropriate in the national security context. In contrast, the minority concluded that the requirement in s.21 that the Minister have a belief on reasonable grounds that the warrant is required to investigate a threat to the security of Canada was "so broad as to provide no objective standard at all. Even when due account is taken of the importance of the state interest involved, the extent of the possible intrusion on the privacy of the citizen is wholly disproportionate."[171]

There are few public cases decided under s.21 of the *CSIS Act*. The Canadian Civil Liberties Association challenged s.21 on the basis that it allowed intrusive investigation of activities that were not unlawful, but defined in s.2 of the *Act* as threats to the security of Canada. Potts J. rejected these arguments primarily on the basis of the decision of the majority of the

---

170 ibid at 198.
171 Ibid at 199.

Federal Court of Appeal in *Atwal*. He concluded that the investigative powers of CSIS did not in either their purpose or effect violate any of the fundamental freedoms under s.2 of the Charter. Potts J. held there was no violation of s.8 of the Charter because there was no reasonable expectation of privacy with respect to lawful advocacy or protest conducted in public. In addition, s.21 provided for prior judicial authorization of searches on the basis of objective criteria and sworn evidence. [172] The Ontario Court of Appeal in a decision by Charron J.A. dismissed an appeal on the basis that the Canadian Civil Liberties Association did not have public interest standing because directly affected people could, as in *Atwal*, litigate the issue. Abella J.A. dissented with respect to standing, but would have dismissed the CCLA's appeal on the merits because of a failure to establish an evidentiary basis for the violation.[173] The fact that the issue in *Atwal* has not been re-litigated in the last twenty years, however, suggests that regular attempts have not been made to admit evidence from CSIS wiretaps in criminal trials.

A few cases have been litigated in the Federal Court about the proper administration of s.21 warrants. One such case involved an attempt by CSIS to obtain authorization for a CSIS employee, the Director General of Counter-Terrorism, to substitute a foreign visitor for a previous target of the CSIS warrant. The Federal Court rejected this request as inconsistent with the purposes of s.21 in ensuring that there is judicial authorization of electronic surveillance under the *Act*. McGillis J. stressed the judicial role in authorizing CSIS warrants by concluding that a substitution authorized by the Director General was not authorized in the *CSIS Act* and would, in any event, " offend the minimum constitutional requirement in *Hunter et al v. Southam Inc.*, supra, in that it would empower a Service employee, who, by the very nature of his position acts in an investigative and not in an adjudicative capacity, to assess evidence and to apply the full range of the intrusive powers in the warrant against a person." [174] If there was evidence available to convince a CSIS employee that a visitor presented a threat to the security of Canada "that evidence is equally available to be placed before a judge on an emergency application. Indeed, a judge is on duty, twenty-four hours a day, to hear precisely such matters. The fact that it may be more expedient for a Service employee to perform the function is patently irrelevant."[175] This case underlines the importance of

---

172 (1992), 8 O.R. (3d) 289 at paras 101, 116 (Gen.Div.)
173 *Canadian Civil Liberties Association. v. Canada* (1998) 126 C.C.C.(3d) 257 at para 109 (Ont.C.A.)
174 *Re Canada Security Intelligence* Act [1997] F.C.J. no. 1228 at para 10 (F.C.T.D.)
175 ibid at para 11

judicial authorization of a CSIS warrant; a prime factor should the state attempt, in future terrorism prosecutions, to use information obtained from a CSIS warrant in a criminal trial.

Does the CSIS warrant scheme violate s.8 of the Charter? The Federal Court of Appeal split 2:1 on this issue in 1987 and there has not been a definitive adjudication of the issue since that time. Although Charter jurisprudence has evolved considerably since 1987, the basic issues debated in *Atwal* still define the parameters of the debate. The central issue continues to be whether *Hunter v. Southam* crime standards apply to security intelligence intercepts. *Hunter v. Southam* itself, however, contemplated that different standards could apply with respect to national security matters. Although it does not require full *Hunter v. Southam* standards, the CSIS scheme provides some protection for privacy through the requirement of judicial authorization, including the requirement under s.21(2)(b) that less intrusive investigative means will not be successful. In addition, the courts have generally not required crime-based reasonable grounds standards for legitimate regulatory searches. On the other hand, it could be argued that *Hunter v. Southam* crime-based standards should apply if the results of a CSIS wiretap are to be introduced in a criminal trial or when CSIS is focusing its investigations on individuals who may be guilty of terrorism crimes. Even if CSIS wiretaps were obtained in violation of s.8, they could still be defended as a reasonable limit under s.1 of the Charter.

2. Section 1 of the Charter

A section 1 defence of the CSIS warrant scheme would likely focus on the role of security intelligence in providing governments with advance information that could be used to prevent acts of terrorism. Such an objective is pressing and substantial and the CSIS warrant scheme, which requires less than probable cause of a crime, is rationally connected to the objective of prevention. The critical s.1 questions would be whether there was a reasonable alternative that was more respectful of s.8 rights and the overall balance between the harm to a person's rights and the benefits of the CSIS warrant scheme. In this analysis, concerns could be raised that the CSIS warrant scheme is overbroad.

CSIS's terrorism mandate is focused on "activities within or relating to Canada directed toward or in support of the 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."[176] The focus in this section is on serious violence towards persons or property. The inclusion of serious violence to property is broader than the definition of terrorist activity in s.83.01 of the Criminal Code which is limited to "substantial property damage" that "is likely to result" in danger or serious bodily harm to a person, serious risk to health or safety or endangerment of human life. It could be argued, however, that the preventive and non law-enforcement mandate of CSIS justifies its broader mandate with respect to property damage.

In addition, a trial judge has found that the reference to terrorist activities being for the purpose of achieving a political, religious, or ideological purpose, objective or cause, in s.83.01 of the Criminal Code, constituted an unjustified violation of the fundamental freedoms.[177] The Special Senate Committee conducting the three-year review of the Anti-Terrorism Act has also recommended that the reference to political, religious or ideological purpose be removed from the *CSIS Act*, and replaced with more neutral language that focuses on actions designed to intimidate a population or compel a government or international organization to act.[178] At the same time, the Commons committee conducting its own three year review made no similar recommendation.[179]

Another potential overbreadth challenge to the definition of threats to the security of Canada in the *CSIS Act* is that it includes lawful advocacy, protest or dissent, if carried on in conjunction with activities that constitute threats to the security of Canada. The ATA contains a broader exemption for "advocacy, protest or stoppage of work", so long as it is not intended to endanger life, public health or safety, or cause death or serious bodily harm. The more limited CSIS exemption could, however, be defended on the basis that it does not criminalize activity, but only defines the investigative and intelligence mandate of a security intelligence agency that does not have police powers.

Evidence obtained under a CSIS wiretap would qualify as a search that was authorized by law and, barring problems with the affidavits or the administration of the warrant, as a search that was conducted in a

---

176 *CSIS Act* s.2
177 *R. v. Khawaja* (2006) 214 C.C.C.(3d) 399 (Ont.Sup.Ct.)
178 Special Senate Committee on the *Anti-Terrorism Act Fundamental Justice in Extraordinary Times: Main Report of the Special Senate Committee on the* Anti-Terrorism Act February, 2007
179 *Rights, Limits, Security: A Comprehensive Review of the Anti-Terrorism Act and Related Issues* March 2007

reasonable manner. In addition, investigative necessity must be shown to obtain a CSIS warrant whereas it now does not have to be demonstrated to obtain a Criminal Code warrant in a terrorism investigation. Following the majority decision in *Atwal*, courts might find that the law is reasonable given the role of an intelligence agency.

If evidence obtained through a CSIS wiretap was sought to be introduced in a criminal trial, however, it would be important for the state to establish that the CSIS wiretap process was not being used as a shortcut around Criminal Code authorizations. Stanley Cohen has suggested that the courts might rely on a trilogy of cases taken from the field of regulatory inspections and searches. This analysis would suggest that a CSIS search could be reasonable if the predominant purpose of the search was not the determination of penal liability but rather the legitimate "regulatory" goals of CSIS in investigating threats to the security of Canada. The test for determining when "the officials 'cross the Rubicon'", and "the inquiry in question engages the adversarial relationship between the taxpayer and the state", is when "the predominant purpose of the inquiry in question is the determination of penal liability."[180]

The test to determine when criminal law standards should apply is not a bright line one, but depends on the totality of the circumstances. The line will not be crossed simply because there are reasonable grounds or a suspicion that an offence may have occurred. At the same time, the line may be crossed before actual charges are laid. Relevant factors would include whether there were reasonable grounds to lay charges, whether the state's conduct was consistent with a criminal investigation, the relation between the regulatory officials (in this case CSIS) and criminal investigators and whether the information being collected was relevant to penal liability. Contact between CSIS and the RCMP, while not determinative, would likely count as evidence that the "Rubicon" had been crossed. In addition, the possibility of laying a criminal charge, including new financing, participation and instructing terrorist activities offences, might also count as a factor suggesting that an attempt had been made to circumvent Criminal Code authorization.

CSIS warrants in terrorism cases should be closely monitored to determine when the line into criminal investigations has been crossed. At that

---

180 See Stanley Cohen *Privacy, Crime and Terror* (Toronto: Lexus Nexus 2006) at 399-402 *R. v. Jarvis* [2002] 3 S.C.R. 757 at para 88

point, a Criminal Code warrant should be obtained because the Court has stressed that "wherever the predominant purpose of an inquiry or question is the determination of penal liability, criminal investigatory techniques must be used. As a corollary, all Charter protections that are relevant in the criminal context must apply."[181]

3. Section 24(2) of the Charter

Even if evidence obtained from a CSIS wiretap were to be found to violate s. 8 of the Charter and not to be justified under s.1 of the Charter, the evidence could still be admissible under s.24(2) of the Charter. Section 24(2) of the Charter provides that unconstitutionally obtained evidence shall be excluded if its admission in all the circumstances would bring the administration of justice into disrepute. The Court has drawn a distinction between the admission of unconstitutionally obtained evidence conscripted from the accused and evidence that was not so conscripted. The admission of conscriptive evidence will generally affect the fairness of the trial and require exclusion, while non-conscriptive evidence will only be excluded after balancing the seriousness of the violation against the adverse effects of excluding the evidence.[182]

In *R. v. Duarte* [183], the Court admitted wiretap evidence despite finding that it was obtained in violation of s.8 of the Charter. It did not invoke the fair trial test, and instead held that the admission of the evidence would not bring the administration into disrepute because the police acted in good faith reliance on a statute that was presumed to be valid in exempting participant surveillance from the warrant requirements in the Code. In 1995, the Court again admitted evidence obtained from electronic participant surveillance conducted in violation of s.8. The Court concluded that it "seems readily apparent that the admission of the evidence did not affect the fairness of the trial. The appellant could not by any stretch of the imagination be said to have been conscripted into incriminating himself in these conversations". [184] Other courts have held that the same rationale applies to unconstitutional third party electronic surveillance on the basis that while the accused's statements were recorded by the state, they were made independently of state intervention.[185]

---

181 ibid at para 98
182 *R. v. Stillman* [1997] 1 S.C.R. 607.
183 [1990] 1 S.C.R. 30.
184 *R. v. Wijesinha* [1995] 3 S.C.R. 422 at para 55.
185 *R. v. Pope* (1998) 129 C.C.C.(3d) 59 at para 8 (Alta.C.A.).

Even if obtained through an unjustified violation of s.8 of the Charter, evidence obtained under a CSIS warrant will likely be held to be non-conscriptive evidence. Its admissibility would then depend on a balancing of the seriousness of a violation against the adverse effects of admitting evidence. Good faith reliance on statutes and warrants has been held, in many cases, to mitigate the seriousness of the violation.[186] The importance of the evidence to the case and the seriousness of the charges have been held to increase the adverse effects to the administration of justice of excluding even unconstitutionally obtained evidence.

In the Air India prosecution, Justice Josephson ruled that even though a search warrant executed against Mr. Reyat violated s.8 of the Charter because it did not specify any time limit on the search, it was nevertheless admissible under s.24(2) because the admission of the evidence would not affect the fairness of the trial, and the violation was not serious. Although he found no s.8 violation in relation to a misdescription in the affidavit of CSIS wiretaps as a confidential and reliable source that could not be revealed for security reasons, it is possible that he would have found that any violation resulting from this approach did not require exclusion under s.24(2) of the Charter in order to avoid condoning a serious Charter violation.[187] This decision affirms the important role that s.24(2) could play in an individual case. That said, s.24(2) would be a finite resource when it comes to the admission of CSIS intelligence in criminal trials, because it will become more difficult over time for the government to argue that it acted in good faith reliance on the CSIS warrant scheme if it has been found to violate the Charter.

4. Use and Disclosure of a CSIS Warrant: A Case Study of R. v. Atwal

The following case study demonstrates that CSIS wiretaps could be admitted at a criminal terrorism trial, but also that the consequence of

---

186 See for example *R. v. Fliss* [2002] 1 S.C.R. 535 and cases reviewed at Roach *Constitutional Remedies in Canada* (Aurora: Canada Law Book, 2006) at 10.1576-10.1647.

187 He stated that he "would not have characterized the drafting technique employed in the unique circumstances of this case as a 'deliberate deception'. That phrase connotes a sense of fraud and dishonesty. I accept that the informant was at the mercy of C.S.I.S. in crafting the information to obtain. C.S.I.S. was a new organization in 1985. The interrelationship between the R.C.M.P. and C.S.I.S. was undefined and the source of some confusion in relation to the Air India investigation. While I cannot assess the reasonableness of the insistence by C.S.I.S. that its involvement not be disclosed, the informant was left with little choice but to accept that condition. The alternative was not to use any of the evidence gathered by C.S.I.S., which would have substantially affected the likelihood of obtaining the search warrants sought. Faced with that dilemma, they proceeded in this reasonable fashion. The use of language obscuring the involvement of C.S.I.S. was, like many other elements in this case, unprecedented, unique, and unlikely to re-occur." *R. v. Malik* 2002 BCSC 1731 at para 71

such admission would be disclosure of the material used to obtain the warrant. As will be seen, the CSIS wiretap evidence in this case was never used in a criminal trial. This was not because of problems with respect to the constitutionality of the CSIS warrant scheme, but rather because of problems with respect to false and misleading information in the affidavit used to obtain the particular warrant.

Four accused Sikh men were charged with attempted murder after the shooting in British Columbia on May 25, 1986, of Mr. Malkiad Singh Sidhu, the Minister of Planning for the state of Punjab in India, upon a visit to British Columbia. These men were apprehended, not because of CSIS information or wiretaps, but rather because they were apprehended by the police shortly after the shooting. The four accused were found guilty by a jury of the attempted murder charge on February 27, 1987. The Crown's case relied on physical evidence connecting the four men with a car that had been abandoned at the scene of the shooting.[188] The four men were each sentenced to 20 years in prison. This sentence was subsequently upheld on appeal to the British Columbia Court of Appeal, in part on the basis of life imprisonment sentences given in 1986 for two men convicted of conspiring to blow up an Air India plane. [189]

Charges of conspiracy to commit murder were subsequently laid in September, 1986 against the same four men and five other men including Harjit Singh Atwal after CSIS revealed incriminating wiretaps to the police about a plot to kill Mr. Sidhu. The conspiracy charge was severed from the attempted murder charge against the four men arrested at the scene. This decision was, in part, because of the complexities of different evidentiary standards that might apply to the different offences.[190] It also reveals how choice of charge in some case may affect the need to use intelligence in a criminal trial. The conspiracy charge was based on the CSIS wiretaps, but the attempted murder charge was based on physical evidence.

The remaining conspiracy charge collapsed and was stayed by the Crown after CSIS officials indicated that misleading information had been included in the affidavit used to obtain a warrant under s.21 of the

---

188 *R. v. Dhindsa* [1989] B.C.J. no. 2194 denying appeals from conviction. The RCMP's arrest of the four perpetrators was not apparently related to the incriminating information that was discovered through the CSIS wiretap. There were reports at the time that CSIS did not inform the RCMP of the threats against the visiting Indian cabinet minister. Neil Macdonald "Spy Agency kept Indian Minister's visit secret from RCMP" Ottawa Citizen Sept. 15, 1987 A1.

189 *R. v. Atwal* [1990] B.C.J. no. 1526.

190 *R. v. Atwal* [1987] B.C.J. No. 397.A change of venue was also granted to New Westminister.

CSIS Act.[191] The Crown had prepared to use evidence obtained under the broadly worded CSIS warrant. The CSIS warrant applied, not only to Atwal's home, but other places that he might resort to. [192] Atwal had applied to the Federal Court that issued the warrant to rescind the warrant. The issuing judge refused to rescind the warrant. On appeal, the Federal Court of Appeal held 2:1 that s.21 of the *CSIS Act* did not violate s.8 of the Charter. As discussed above, the Court of Appeal rejected various facial challenges to the warrant in part on the basis that inferences could be made that the judge had addressed the necessary criteria under s.21(2)(a) and (b) of the act. It also relied on American authority that held that "domestic security surveillance may involve different policy and practical considerations from the surveillance of 'ordinary crime'. The gathering of security intelligence is often long range, and involves the interrelation of various sources and types of information…the emphasis on domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crime."[193]

The Court of Appeal reversed the issuing judge's order that the affidavit used to obtain the CSIS warrant not be disclosed. The trial judge had denied disclosure of the affidavit on the basis that the affidavit:

> …relates to political terrorism which was in the course of being investigated in the interests of national security. Disclosure might well result in the revelation of security investigatory methodology which could lead to the significant impairment of the effectiveness of this and future security investigations. The public interest in protecting and preserving the security service's ability to discharge the onerous and important mandate given to it under the C.S.I.S. Act in the interests of national security cannot be disregarded or ignored.[194]

Mahoney J. for the Federal Court of Appeal rejected this argument on the basis that "the ends of national security are not tantamount to the ends

---

191 The disclosure led to Ted Finn, the first director of CSIS, resigning. When two of the men charged were released from prison they were greeted by Talwinder Singh Parmar. Kim Bolan "Separatist slogans welcome free Sikhs" Vancouver Sun Sept 16, 1987 E8.

192 Terry Glavin "Eavesdropping legality upheld" Vancouver Sun May 1 1987 A11.

193 *R. v. Atwal*(1987) 36 C.C.C.(3d) 161 at 178 quoting *U.S. v. U.S. District Court* 407 U.S. 292 at 322 (1972).

194 ibid at 189

of justice". [195] He reasoned that the accused's entitlement to challenge the affidavit should not be different from those that would apply to the accused at trial. Although intelligence obtained through CSIS warrants might in some cases be used as evidence, full disclosure of the intelligence, as well as the basis for obtaining the intelligence, may be the price that is paid for admissibility of intelligence as evidence.

The disclosure ordered by the Federal Court of Appeal was not absolute. It indicated that "the only statutory limitation on disclosure is an absolute prohibition against disclosure by any person of information from which the identity of an informer or an employee engaged in covert operations can be inferred. That prohibition should be respected by the court."[196] The Court of Appeal ordered that the judge who issued the warrant should disclose the affidavit to Atwal "after deleting therefrom anything from which the identity of any person described in s. 18(1)(a) and/or (b) of the Act can be inferred"[197]. In addition, this disclosure was made subject to the ability of the Attorney General to claim public interest immunity under the *Canada Evidence Act*. Such claims were not made. In any event, the wiretap evidence was never tendered by the Crown at any trial. The warrant was rescinded when the Attorney General of Canada revealed that false information had been used to obtain the warrant. The provincial Attorney General declined to proceed with the case. Although it could be argued that even unwarranted intercepts could be admitted as evidence under s.24(2), it would have been difficult to argue that the Charter violation was not serious or was committed in good faith in light of the concessions that the affidavit used to obtain the CSIS warrant was inaccurate.

The *Atwal* case study demonstrates that evidence obtained under a CSIS wiretap could in some cases be used in criminal trials. It is, however, possible that the accused might have been able to object to the warrant, including its broad resort to clause, before the trial judge, had the wiretap evidence been tendered at trial. The argument would have been that even if the CSIS warrant was reasonable on its face, that the breadth and the manner of the search would have been unreasonable. The extensive litigation in the Federal Court over the warrant would not have necessarily settled the question of the admissibility of the warrant at trial. That said,

---

195 ibid at 190

196 ibid at 186. This was a reference to the restrictions on disclosure under s.18(1) of the *CSIS Act*. This restriction is, however, subject to the authorized grounds of disclosure under s.19 including disclosures to police and Attorneys General with respect to investigations and prosecutions.

197 Ibid at 192

a trial judge would have the option of admitting evidence from a CSIS wiretap under s.24(2), even if the evidence was obtained in violation of s.8 of the Charter and the violation was not justified under s.1.

The attempt to use the CSIS wiretap as evidence allowed the accused both to challenge the CSIS warrant scheme and the breadth of the particular warrant under the Charter. The fact that the CSIS scheme will attract Charter challenge may make it advisable, if possible, to use Criminal Code wiretap warrants that have been repeatedly upheld under the Charter. That said, the structure of the Charter allows the state several opportunities to justify the use of CSIS wiretaps in criminal trials. As discussed above, even if s.21 of the *CSIS Act* violates s.8 of the Charter, the government can argue that it is a reasonable limit on the right. Even if this argument fails, the government can argue that the wiretap evidence is admissible under s.24(2) of the Charter as non-conscriptive evidence that was obtained in good faith reliance on a valid statute and a valid warrant. The good faith argument was not available in *Atwal*, but more because of particular circumstances of the case that are not likely to be repeated.

The *Atwal* case study demonstrates that disclosure may be the price paid for the evidentiary use of intelligence. The Federal Court of Appeal unanimously concluded that the affidavit in support of the CSIS warrant should be disclosed to the accused to allow the accused to challenge the legality and constitutionality of the warrant. As will be seen in the subsequent discussion of the *Parmar* case study, disclosure of such information mirrors standards of disclosure used with respect to Criminal Code wiretap warrants. The initial engagements of CSIS with the criminal justice system and its disclosure obligations were not happy experiences for CSIS. They may have influenced CSIS attitudes towards engagement with the criminal justice system. That said, CSIS, like its peer agencies such as MI5, must be prepared for the fact that intelligence gathered in its terrorism investigations may in some cases be used as evidence.

Although disclosure is necessary to respect the accused's right to full answer and defence and to challenge the legality and constitutionality of the search, it is not an absolute value. The Court of Appeal indicated that the confidential affidavit containing intelligence that was used to obtain the warrant could be edited to respect s.18 of the *CSIS Act* so as not to reveal the identity of confidential sources of information or any CSIS employee engaged in covert operational activities. A corollary

of such editing, however, would be that information edited out of the affidavit and not disclosed to the accused could not be used to support the warrant. Depending on how the affidavit was constructed, editing out material could result in a conclusion that the warrant was not legally or constitutionally granted. As will be seen, this is what happened in the *Parmar* case. That said, the affidavits used in *Atwal* and *Parmar* were drafted at a time when the accused had not gained access to the sealed packet of confidential material used to obtain wiretap warrants. Today, the affidavits would be drafted with the possibility of editing to protect public interests in non-disclosure in mind. In any event, even if the CSIS warrant in *Atwal* could not be upheld as consistent with s.8 of the Charter once information that could identify confidential informants or covert agents was edited out, the state could still argue that the unconstitutionally obtained evidence could be admitted under s.24(2).

Although the Federal Court of Appeal unanimously ordered that the affidavit used to obtain the warrant should be disclosed to the accused, it was not blind to the dangers of disclosing intelligence. As discussed above, it contemplated that the affidavit would be edited to protect confidential informants and covert agents. It also noted that the Attorney General of Canada could apply under what is now ss.37 or 38 of the *Canada Evidence Act* to obtain a non-disclosure order on the basis of harms to national security and other public interests. Such orders would also mean that the warrant could not be supported by confidential information that was the subject of a non-disclosure order, and the admissibility of the evidence might have to be determined under s.24(2). As will be examined below, the process of applying for a non-disclosure order under s.38 of the CEA would require separate litigation in the Federal Court.

The *Atwal* case study demonstrates that the evidentiary use of intelligence may come with the price of disclosure to the accused. Disclosure is not, however, absolute. Affidavits containing intelligence can be edited before disclosure to the accused and non-disclosure orders can be sought through separate litigation under the CEA. Material that is edited out of the affidavit and not disclosed to the accused cannot be used to support the warrant. At the same time, the state can argue, in the absence of other improprieties such as the inaccuracies in the affidavit in *Atwal*, that electronic surveillance, even that obtained under an unconstitutional wiretap, could still be used as evidence under s.24(2) of the Charter.

5. Summary on the Admission of CSIS Wiretaps

Although it is 20 years old, the Federal Court of Appeal's decision in *Atwal* is still the leading precedent holding the CSIS warrant scheme to be constitutional. Such a conclusion would require courts to accept the distinct purpose of intelligence gathering as opposed to law enforcement either when interpreting s.8 of the Charter or under s.1 of the Charter. Courts may be more inclined to find a Charter violation if they are persuaded that CSIS "crossed the Rubicon" by focusing on the penal liability of specific individuals. Even then, however, evidence obtained through a CSIS warrant might still be admitted under s.24(2) on the basis that the admission of unconstitutionally obtained evidence obtained in good faith reliance on legislation and a warrant would not bring the administration of justice into disrepute.

The Federal Court of Appeal's decision in *Atwal* also affirms that the disclosure of the affidavit used to obtain the CSIS warrant will be required to allow the accused to challenge the warrant as part of the right to make full answer and defence. Disclosure is not absolute, because the affidavit can be edited to protect confidential sources and covert agents, and because and the Attorney General of Canada can make national security confidentiality claims.

C) The Case for Earlier Use of Criminal Code Electronic Surveillance Warrants

Any assessment of the constitutionality of the CSIS wiretap warrant scheme cannot be undertaken in the abstract. In deciding whether a particular CSIS wiretap violates the Charter, courts are likely to ask whether grounds existed for obtaining a Criminal Code wiretap warrant. When intelligence is being collected, security intelligence agencies must ask themselves whether they have "crossed the Rubicon" into a predominant focus on criminal liability. Although this test is a flexible one that depends on all the circumstances and will not be triggered simply by discussions with the police, or even by the existence of reasonable grounds to believe that a crime has been committed, it is a question that should be asked at regular intervals during counter-terrorism investigations. If at all possible, the state should not rely on complex after-the-fact adjudications on whether a line has been crossed, or about the possibility that security intelligence may be found to be admissible in a criminal trial under s.24(2) of the Charter. In cases of uncertainty, but where there are sufficient

grounds for a Criminal Code authorization, preference should be given to the collection of evidence under Criminal Code warrants. Such a process will, however, require close co-operation between CSIS and the police. Information obtained by the police from Criminal Code warrants that has intelligence value can always be passed on to the security intelligence agencies, whereas the passing of information obtained by CSIS to the police has been more problematic in the past.[198]

The 2001 *Anti-Terrorism Act* amendments have made Criminal Code electronic surveillance warrants more attractive from the state's perspective. Criminal Code warrants in terrorism investigations can now, like CSIS wiretap warrants, be issued for up to a year. [199] Unlike CSIS warrants[200], there is no longer a requirement of establishing that other investigative procedures such as surveillance, informers, undercover agents and regular search warrants would not be successful in order to obtain a Criminal Code warrant in relation to a terrorism investigation.[201] Finally, the grounds for warrants obtained under *Hunter v. Southam* crime-based standards have expanded with the enactment of many new terrorist crimes that apply long before an actual act of terrorism has occurred. Although it has always had a preventive dimension, as represented by the law of conspiracy and attempts, the ATA has created many new crimes relating to support, financing, participation and preparation for acts of terrorism.[202]

The domains of intelligence and evidence collection are shifting both because of the availability of new crimes and legislative changes that make it easier to obtain Criminal Code authorizations for electronic surveillance in terrorism prosecutions. The result may be that some investigations in which a warrant under s.21 of the *CSIS Act* would have been used can now from the start be conducted under a Criminal Code authorization.

The use of Criminal Code warrants is not a panacea. The next case study underlines how disclosure issues led to the collapse of a terrorism prosecution of a person who is widely believed to have been the mastermind of the bombing of Air India Flight 182. Although Criminal

198 See the discussion of RCMP and CSIS co-operation in Part 1 of this study.
199 Criminal Code s.186.1.
200 *CSIS Act* s.21(5). CSIS warrants in relation to subversion under s.2(d) of the Act are limited to sixty days.
201 Criminal Code s.186 (1.1). Notification of the target can be delayed up to 3 years under s.196(5) of the Code, though no notification is required for CSIS wiretaps.
202 See infra part 1 for a more detailed discussion of new terrorism crimes.

Code warrants will require the state to establish reasonable grounds to believe that a crime has been, or will be, committed and reasonable grounds that the collection will reveal evidence of the crime, it has become easier to obtain Criminal Code electronic surveillance warrants in terrorism investigations than at the time of the Parmar and Atwal cases discussed in this section. As will be seen, the Parmar case might be decided differently today as a result of Parliament's abolition of an automatic statutory exclusionary rule that applied to unwarranted or unlawful electronic surveillance. Today the state would have a stronger argument that the wiretap evidence should be admitted under s.24(2) of the Charter, even if the need to protect the identity of an informer meant that the edited affidavit could no longer support the warrant. There are also provisions in the Criminal Code that now allow the prosecutor to edit the affidavit used to obtain the warrant in order to protect a wide range of public interests. The accused can only seek more disclosure if the judge determines that a summary would not be sufficient and the material is required for the accused to make full answer and defence.[203]

The jurisprudence and procedures used to challenge Criminal Code warrants and to edit confidential material before it is disclosed to the accused are better established and more certain than the scant jurisprudence surrounding the use of CSIS material in criminal trials. In addition, the legislation providing for Criminal Code wiretaps has been upheld by the Supreme Court,[204] whereas the Federal Court of Appeal in *Atwal* only affirmed the CSIS wiretap provision in a divided decision made over twenty years ago. Where possible, Criminal Code electronic surveillance warrants should be used in counter-terrorism investigations. Intelligence agencies need to constantly explore the relation between their intelligence gathering and comparable collection of evidence by the police.

D) Parmar - A Case Study of Disclosure and Criminal Code Warrants

On June 14, 1986, seven Sikh men were charged in Hamilton with conspiring to commit various violent crimes in India. The alleged plans involved bombing Indian Parliament buildings, derailing trains in India, blowing up an oil refinery in India, as well as kidnapping a child of a member of the Indian Parliament in order to force him to assist them in the above plans. Two accused were discharged, but the remaining men,

---

203 Criminal Code ss.187(4) and 187(7).
204 *R. v. Garofoli* [1990] 2 S.C.R. 1421; *R. v. Thompson* [1990] 2 S.C.R. 1111

including Talwinder Singh Parmar, were ordered to stand trial on three counts of conspiracy on December 22, 1986.

On March 10, 1987, Justice Watt dealt with an application by the accused for an order to open the sealed packets of material (containing two affidavits), which formed the basis for an authorization to intercept private communications. The basis for this application was that it was necessary for the applicants to make full answer and defence to the charges they faced at trial. Watt J. characterized the accused's argument for access to the sealed packet in the following terms:

> It is said that a critical aspect of the right to make full answer and defence, an incident of the constitutional right of fundamental justice guaranteed by s. 7 of the Charter, is the right to challenge the receivability of that portion of the prosecution's proof which is the primary evidence said to have been obtained by interceptions made in accordance with those authorizations and/or renewals the informational basis of which is sought to be disclosed. It would seem that the argument ultimately to be made against the receivability of the primary evidence rests upon a submission that the interception process constituted an unreasonable search or seizure, thereby an infringement of s. 8, and ought to be excluded in accordance with s. 24(2) of the Charter.[205]

Conversely, the Crown argued that opening a sealed packet should be sparingly exercised in light of the statutory provisions for confidentiality. The Crown argued that the accused should demonstrate on the balance of probabilities that access to the sealed packet was required to make full answer and defence.

Justice Watt acknowledged that s.178.14 of the Criminal Code then in force only allowed for breaching the confidentiality of the sealed packet when (a) dealing with an application for renewal of the authorization, and (b) pursuant to an order of a judge. Before the Charter, it was only in exceptional circumstances, such as allegations of fraud or material non-disclosure, that a judge would order that a sealed packet supporting the warrant be opened. Nevertheless, he held that the accused should have access to the sealed packet in order to make a meaningful challenge that

---

205 *R. v. Parmar* (1986) 34 C.C.C.(3d) 260 at 273 (Ont.H.C.)

the warrant violated s.8 of the Charter. Justice Watt found that such an approach did "no violence to the plain wording" of the Code and that it was "further, compatible with the fundamental justice guarantee of the s. 7 of the Charter."[206] He also found that ordering disclosure accords with the strong public policy in favour of openness in respect of judicial acts, even when those acts were initially performed on an *ex parte* and *in camera* basis.[207]

Justice Watt concluded that the accused should have access to the sealed packet that authorized the wiretap warrant on the basis that if the accused were required to demonstrate "fraud or material non- disclosure before an order may issue permitting the opening of the sealed packet, the accused are in a catch-22 situation. In most cases evidence of material non- disclosure in particular will not emerge by magic. It is only upon that access to the sealed packet that the accused will be able to develop a meaningful capacity to advance a defence on this issue."[208] Access to the sealed packet was supported by the accused's right to full answer under s.7 of the Charter, the right against unreasonable search and seizure under s.8 of the Charter, as well as the need for public accountability for a warrant process even though the warrant was initially on an *in camera* and *ex parte* basis.

Justice Watt acknowledged that the accused were being granted access to the sealed packet in the absence of any evidence of wrongdoing in the obtaining of the warrant and that:

---

206 ibid at 276

207 He explained: "It may also be observed that to order disclosure under the relevant subparagraph in the present circumstances, subject to editing, also accords with the strong public policy in favour of openness in respect of judicial acts, even those which have been initially performed on an *ex parte* and *in camera* basis. Whilst it is no doubt true, as has been held in the case of conventional search warrants, that the effective administration of justice would be frustrated in the event that individuals were allowed to be present upon the issuance of investigative warrants in respect of themselves, the force of such argument substantially abates upon the execution of the order. Thereafter, there exists but a diminished or attenuated interest in confidentiality. It is a fortiori when the evidentiary fruits produced by the issuance of such investigative warrant are to be adduced in a public trial. Further, it has been authoritatively held that the strong public policy in favour of openness in respect of judicial acts, such as the issuance of conventional search warrants, contemplates maximum accountability and accessibility. At every stage there ought to be public accessibility and concomitant judicial accountability. The former should only be curtailed in the event of a present need to protect social values of superordinate importance and, in my respectful view, then only to the minimal extent necessary to achieve such purpose:" ibid at 278

208 ibid at 273 quoting *R. v. Wood* et al. (1986), 26 C.C.C. (3d) 77 at 87-88.

> It may seem somewhat anomalous or incongruous that the mere assertion of a right to fundamental justice, without a scintilla of evidence to support an argument of its denial, should serve as a sufficient basis upon which to breach the statutory secrecy of the sealed packet. Indeed, it may appear to be all the more so when compared to that which is required in the event that fraud or material non-disclosure is asserted as the basis upon which the packet should be opened. It must be recalled, however, that what is being here contested is the right to access to the packet in order to raise a potential challenge upon constitutional grounds that certain evidence ought not to be received. In practical terms, it may, to some extent, be a fishing expedition. It is, however, a fishing expedition in what are now constitutionally-protected waters. The ultimate questions of whether the order should be set aside and whether evidence said to be gathered in accordance therewith ought to be received, are quite other matters. To permit access in the present circumstances is but to construe s.178.14(1)(a)(ii) in a manner compatible with the constitutional guarantee of fundamental justice enshrined in s. 7.[209]

Disclosure was required by the Charter. Even if disclosure could be characterized as "a fishing expedition", it was one conducted in "what are now constitutionally protected waters." Although his decision to grant the accused access to the sealed packet was innovative at the time, it was subsequently followed by the Supreme Court.[210]

The accused's Charter based right to access to the sealed packet was not absolute. As in *Atwal*, some allowance would be made for public interests in non-disclosure. Justice Watt stated it was his duty to review the affidavit, and make any editing changes he felt were necessary in the best interests of the administration of justice. He indicated that he would edit the material before it was disclosed to the accused taking to account factors such as:

> (a) whether the identities of confidential police informants, and consequently their lives and safety, may

---

209 ibid at 279-280
210 *Dersch v. Canada* [1990] 2 S.C.R. 1505

> be compromised, bearing in mind that such disclosure may occur as much by reference to the nature of the information supplied by the confidential source as by the publication of his or her name;
>
> (b) whether the nature and extent of ongoing law enforcement investigations would thereby be compromised;
> (c) whether disclosure would reveal particular intelligence-gathering techniques thereby endangering those engaged therein and prejudicing future investigation of similar offences and the public interest in law enforcement and crime detection, and
>
> (d) whether disclosure would prejudice the interests of innocent persons.
>
> Editing, in my respectful view, ought to take place to the minimal extent necessary to give effect to societal values of superordinate importance thereby ensuring that by its nature and extent it does not, in practical terms, work an equivalent injustice to that which would ensue from an absolute prohibition against disclosure. [211]

After initial editing, the judge would show the edited affidavit to Crown counsel, and if the Crown agreed, he would give a copy to the counsel for the applicants. If further editing was requested, such a determination would be made in open court with the applicants and their counsel present. Defence counsel would not receive a copy until the final editing was done.

The editing procedure used by Justice Watt was subsequently approved of by the Supreme Court in *R. v. Garofoli* [212]and *R. v. Durette*. [213] It was also the basis for amendments to the Criminal Code,[214] which contemplated the opening, and also the editing, of sealed packets. Section 187(4) of the Criminal Code now provides that the information in the sealed packet should not be disclosed to the accused "until the prosecutor has as deleted any part of the copy of the document that the prosecutor believes would be prejudicial to the public interest including any part that the prosecutor believes could:

---

211 *R. v. Parmar* (1986) 34 C.C.C.(3d) 260 at 281-282 (Ont.H.C._
212 [1990] 2 S.C.R. 1421.
213 [1994] 1 S.C.R. 469
214 S.C. 1993 c.40 s.7.

a) compromise the identity of any confidential informant;

b) compromise the nature and extent of ongoing investigations;

c) endanger persons engaged in particular intelligence-gathering techniques and thereby prejudice future investigations in which similar techniques would be used; or

d) prejudice the interests of any innocent person.

The accused can apply to the trial judge for access to material that is edited out but it will only be disclosed under s.187(7) if "required in order for the accused to make full answer and defence" and if "the provision of a judicial summary would not be sufficient". This provision may provide for more extensive editing to protect intelligence than was contemplated by the Federal Court in *Atwal*.

The accused challenged the admissibility of the wiretap evidence at a voir dire conducted at the start of the scheduled trial. During the voir dire, the accused established entitlement to cross-examine the affiant on the affidavit that supported the wiretap on the basis that there was "deliberate falsehood or reckless disregard for the truth" in the affidavit. Justice Watt's decision, which was upheld on appeal to the Ontario Court of Appeal, reveals how warrant practices can be subject to a high level of scrutiny when the fruits of the warrant are sought to be introduced as evidence in a criminal trial.[215]

The errors in the affidavit to support the Parmar warrant were significant. The affidavit alleged that Parmar was connected to the Duncan blast, but "the affiant failed to disclose that on March 24, 1986, three days prior to the affidavit being sworn, Crown counsel had tendered no evidence against the applicant Talwinder Singh Parmar in respect of such a charge."[216] The second error in the affidavit supporting the warrant was that it failed to disclose that extradition proceedings against Parmar for alleged crimes in India were unsuccessful.[217] As in the *Atwal* case discussed above, the disclosure process is a rigourous one which will test the accuracy of the affidavits used to obtain the warrant process.

The wiretap was declared unlawful before the start of the trial largely as a result of a Court of Appeal decision that made clear that reliance could not

---

215 *R. v. Parmar* (1987) 37 C.C.C.(3d) 300 at 319 aff'd (1990) 53 C.C.C.(3d) 489 (Ont.C.A.)
216 ibid at 346
217 ibid at 346

be placed on material that had been edited out by the judge to sustain the wiretap.[218] As with the initial decision to disclose the affidavit, this decision was innovative, but has subsequently become the norm. Justice Watt recognized that this process would apply an "artificial informational basis, the edited affidavit, rather than the material actually before the authorizing judge", but he concluded that it was the only possible procedure that would ensure fairness to both the accused's right to full answer and defence and the Crown's right to protect informers.[219]

Justice Watt concluded "that Crown counsel ought to be afforded the opportunity to persist in non-disclosure yet take the position that the authorization had been properly issued on the basis of the information contained in the affidavit as edited." On the facts of the case, however, the Crown conceded that it could not defend the warrant without the information that was edited to protect the informer. The Crown's decision may in part reflect the fact that the affidavit was drafted at a time when it was expected that it would never be disclosed to the accused or edited. In the result, Watt J. held that Crown counsel had failed to establish that lawful authority existed for the intercept because "the prosecution could not support the issuance of the order without reference to the edited material. The prosecutor's case, accordingly, failed and the accused were found not guilty."[220]

Before the prosecution was ended, however, two alternative methods of reconciling the demands of full answer and defence and public interest immunity, including informer privilege, were considered. The first was that the Crown sought, but was denied, consent from the informer to make necessary disclosures that would reveal his identity. A media story at the time reported that the investigators "could not persuade the informant to make his identity public, Crown Attorney Dean Paquette told the court. The informant rejected an offer to be moved to another community in Canada

---

218 *R. v. Hunter* (1987) 34 C.C.C.(3d) 14 (Ont.C.A.)

219 He elaborated: "It cannot be gainsaid that, to some extent at least, non-disclosure of the type here considered deprives defending counsel of information whereby to test the propriety of the issuance of the authorization, hence reasonableness and constitutionality of the investigative techniques of the state. On the other hand, the imposition of a proportionate or equivalent disability upon the state, namely, denial of reliance upon the non-disclosed information as a basis to support the issuance of the interceptional mandate, ensures that neither advantage is gained by the state nor lost by the accused in the process. The parties are, so nearly as is practically possible, left in a position of equality and as if the non-disclosed material had not been furnished to the authorizing judge. Absent an *in camera ex parte* hearing to examine the impact of the additional non-disclosed material, the present scheme ensures procedural and substantive fairness." *R. v. Parmar* (1987) 31 C.R.R. 256 at 284 (Ont.H.C.)

220 ibid at 284.

under a witness relocation program. Even presenting the defence with a summary of the informant's knowledge would jeopardize the individual's identity… 'No one knows what potential harm could befall the informant should their identity become publicly known,' Paquette told the court '… If I were placed in a similar situation, I would not be prepared to consent to the information identifying me.'[221] The resolution of the Parmar case underlines how issues of disclosure and national security confidentiality are closely connected to the adequacy and attractiveness of witness and source protection.

A second alternative was to draw an adverse inference from the editing process that the wiretap evidence was obtained illegally and without a warrant, but to argue that it should be admissible in any event. This option had recently been recognized by the Ontario Court of Appeal as a possible response to the editing of an affidavit[222] in a regular search warrant case. Justice Watt, however, concluded that "the alternative of a warrantless search in the interception of private communications is of no practical utility in light of the provisions of paragraph 178.16(1) (a) of the Criminal Code." This section of the Criminal Code provided that intercepted private communication were "inadmissible as evidence against the originator of the communication or by the person intended by the originator to receive it unless the interception was lawfully made…" This automatic exclusionary rule has since been repealed.

Today, it would be possible to conclude that the warrant was not valid, but that the wiretap could be admitted under s.24(2) of the Charter without bringing the administration of justice into disrepute. The court would balance the seriousness of the violation of s.8 in intercepting private communications without a valid warrant against the adverse effects on the administration of justice of excluding such evidence. The Crown's case under s.24(2) would be quite strong because the wiretap evidence would constitute non-conscriptive evidence that would not affect the fairness of the trial. Moreover, the evidence was obtained in apparent good faith reliance on a warrant issued under a valid statute. The errors in the affidavit, however, as in *Atwal*, would provide a basis to argue that admitting the product of the warrant would condone a serious violation of the Charter. Under the serious violation test, however, the Crown could stress the adverse effects to the administration of justice of excluding important and perhaps crucial evidence in a case where most serious

---

221 Brian McAndrews "Five acquitted in terror trial" *Toronto Star* April 15, 1987 p.A1.
222 *R. v. Hunter* (1987) 34 C.C.C.(3d) 14 (Ont.C.A.)

crimes were alleged to have been committed. In any event, the option of arguing that the wiretap evidence should be admitted under s.24(2) was, however, precluded in the *Parmar* case because of the automatic exclusionary rule under then section 178.16(1)(a) of the Criminal Code.

Today, *Parmar* might be decided differently. The Crown would argue that even if the warrant could not be supported on the basis of the edited affidavit, evidence obtained under it should be admitted under s.24(2) of the Charter without bringing the administration of justice into disrepute. Today, the underlying affidavit for the wiretap might be drafted differently because the authorities would be aware both that the affidavit may be disclosed and that reliance could not be placed on portions of the affidavit that were edited out to protect informants or other public interests in non-disclosure. Section 187(4) provides broad grounds for editing the affidavit before it is disclosed to the accused and subsequent disclosure will only be ordered under section 187(7) if judicial summaries are not sufficient and the information is required in order for the accused to make full answer and defence.[223] Material that is edited out, however, cannot be used to support the validity of the warrant. When it became apparent that the warrant could not be sustained without revealing the informant's identity, the informant in *Parmar* apparently vetoed the disclosure of his or her identity. *Parmar* demonstrates how disclosure is closely linked to the adequacy, or perceived adequacy, and the attractiveness of witness and source protection programs.

E. Disclosure and the Use of Special Advocates in Challenging Criminal Code and CSIS Warrants

The *Parmar* and *Atwal* case studies reveal how wiretaps can obtain important evidence in terrorism investigations, but that attempts to use such information as evidence will require considerable disclosure to the accused and a high degree of scrutiny of state conduct in obtaining the evidence. Whether warrants are issued under the *CSIS Act* or the *Criminal Code*, the state may be faced with the prospect of revealing the identity of key informants and of having those who swear affidavits in support of a warrant cross-examined on the accuracy and truthfulness of the material that supports the warrant. Both case studies reveal how disclosure standards challenged terrorism prosecutions long before the 1991

223 There may, however, be a case for expanding s.187(4)(c) to allow the protection of all secret intelligence gathering techniques even when disclosure might not endanger the person engaged in the technique.

decision in *Stinchcombe*. The demands of disclosure were not, however, absolute and in both cases, tha affidavits would have been edited to protect confidential sources and ongoing operations before being disclosed to the accused. At the same time, information edited out from the affidavit could not be used to support the wiretap authorization.

There may be other ways to reconcile the interests of the accused in challenging the legality and constitutionality of CSIS or Criminal Code warrants and protecting the confidentiality of information used to obtain the warrant including information from informants, information received in confidence from other agencies and information relating to ongoing investigations. The law at present allows the affidavit to be edited to protect state interests in non-disclosure, but then holds that the state cannot rely on material that is edited out of the affidavit to support the warrant because the accused will not have an opportunity to see and challenge the information. The Supreme Court in the warrant context has stressed the importance of the accused's ability to challenge the warrant as part of the accused's right to full answer and defence.[224] At the same time, the Supreme Court in other contexts has recognized that there may be alternatives to disclosure to the accused that still allow effective adversarial challenge of the state's case and that comply with s.7 of the Charter or constitute a reasonable limit under s.1 of the Charter.[225]

One of these alternatives may be the use of special advocates who because they are security cleared and permanently bound to secrecy could have access to the entire affidavit used to obtain a CSIS or a Criminal Code warrant without editing. The special advocate could then stand in for the accused and provide adversarial challenge to the warrant by arguing that the warrant was illegally and unconstitutionally obtained and the evidence should be excluded. If necessary, the special advocate could have access to the disclosure provided to the accused and demand further disclosure and cross-examine officials on the basis of the affidavit. The Supreme Court has recognized that while a challenge to a warrant is part of the accused's right to fair answer and defence, it is nevertheless a review that is distinct from a trial on the merits. As Charron J. has explained:

> At trial, the guilt or innocence of the accused is at stake. The Crown bears the burden of proving its case

---

224 *R. v. Garofoli* [1990] 2 S.C.R. 14121; *R v. Durette* [1994] 1 S.C.R. 469; *R. v. Pires* [2005] 3 S.C.R. 343.
225 *Charkaoui v. Canada* [2007] 1 S.C.R. 350

> 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 *Garofoli* 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 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 on a *Garofoli* hearing 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.[226]

The limited nature of the challenge to wiretap warrants opens up the possibility that the use of a special advocate to challenge the warrant could be an adequate substitute for allowing the accused to challenge the warrant on the basis of the affidavit as edited to protect the state's interests in secrecy. Such an approach will not and should not guarantee that the fruits of CSIS and Criminal Code wiretaps will always be admissible. The special advocate may be able to demonstrate that the warrant was illegally or unconstitutionally obtained or administered and that exclusion of the

---

226 *R. v. Pires; R. v. Lising* [2005] 3 S.C.R. 343 at paras 29-30.

evidence is necessary to avoid condoning a serious Charter violation that will bring the administration into disrepute. Both the warrants in *Atwal* and *Parmar* had serious flaws. Nevertheless, the use of a special advocate will allow the warrant to be both defended and challenged on the basis of the full record, including material that would today be edited out to protect the state's interests in avoiding disclosure of information about confidential informants and ongoing investigations.

F) The Collection and Retention of Intelligence under Section 12 of the CSIS Act

Apart from the issues of electronic surveillance discussed above, there are questions about whether the methods CSIS uses to collect and retain intelligence affect the possible use of intelligence as evidence. Section 12 of the *CSIS Act* provides:

> 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 and advise the Government of Canada.

As will be seen, this section raises distinct issues about the collection and the retention of intelligence.

Section 12 could be challenged under the Charter either on its own or when information and intelligence that CSIS originally collected is sought to be introduced as evidence in a criminal trial. A threshold issue would be whether CSIS's investigation or actions invaded a reasonable expectation of privacy. The courts might hold that open source material, at least as it is related to material that is not related to a biographical core of information, does not infringe a reasonable expectation of privacy.[227]

If *CSIS* actions affected a reasonable expectation of privacy, any resulting activity would constitute a search under s.8 of the Charter. Such searches would have to be authorized by law; by a law that was reasonable, and

---

227 *R. v. Plant* [1993] 3 S.C.R. 281*; R v. Tessling* [2004] 4 S.C.R. 432

be conducted in a reasonable manner.[228] Section 12 would constitute legal authorization as long as there were, as required under the statute, reasonable grounds to suspect that the activities constituted threats to the security of Canada and the collection of the information was "strictly necessary".

Section 12 of the *CSIS Act* only requires reasonable suspicion of threats to the security of Canada as opposed to reasonable grounds in relation to crime and evidence of crime. Moreover, it does not require judicial authorization of the investigation. As such, intelligence collected under this provision could be found to violate s.8 of the Charter if the courts applied a *Hunter v. Southam* criminal law standard. On the other hand, the courts might find that information collected under this section to be a legitimate exercise of regulatory powers to collect intelligence. This argument would be the strongest in contexts in which authorities had not, as discussed above, "crossed the Rubicon" and assumed the predominant purpose of determining criminal liability.

The requirement in s.12 that CSIS only collect information "to the extent that is strictly necessary" would also help strengthen the argument that s.12 does not violate s.8 of the Charter. As with the use of evidence obtained under s.21 warrants, the use of s.12 evidence would come with the price of disclosure. The accused would be allowed to challenge the legality and constitutionality of the manner in which CSIS obtained the information. The defence would likely also have access to information that was relevant to the reliability of the information.

To the extent that the intelligence was based on hearsay, the courts would determine in a case-by-case manner which material was sufficiently reliable and necessary to justify its introduction in the criminal trial.[229] The determination of the reliability of the evidence would likely require consideration of the conditions under which the intelligence was obtained. Evidence obtained as a result of torture would be inadmissible even if the torture was committed by other parties, but the status of evidence derived from torture is less clear.[230] The fact that intelligence was confirmed by other facts might support admissibility.[231] The consideration of the necessity of introducing the intelligence in a criminal trial could also require consideration of why the evidence was collected by CSIS and not police investigators. Information obtained by CSIS in a regulatory

228 *R. v. Collins* [1987] 1 S.C.R. 265.
229 *R. v. Starr* [2000] 2 S.C.R. 144
230 *A. v. Secretary of State* 2005 UKHL 71; Criminal Code s.269.1(4).
231 *R. v. Khelawan* [2006] 2 S.C.R. 787.

manner that did not focus on the criminality of individual people might be easier to admit than investigations that focused on the determination of penal liability.

The restrictive statutory standard that the collection of the information is "strictly necessary" limits the collection of information. Once that information is collected, however, CSIS has separate obligations to subject the information to analysis and to retain the information. These separate requirements of analysis and retention appear not to be subject to the "strictly necessary" qualification. Indeed, analysis beyond what is "strictly necessary" is to be preferred. At the same time, information should not be retained if its collection was not "strictly necessary" or was otherwise unlawful. As will be seen in the next part of this study, there can also be a duty under s.7 of the Charter to retain information, including intelligence, which should be disclosed to the accused.

It could be argued that the destruction of intelligence such as CSIS wiretaps or notes taken by CSIS agents is supported by the requirement in s.12 of the *CSIS Act* that information should only be collected "to the extent that is strictly necessary". Contrary to such arguments, the words "strictly necessary" qualify the reference to investigation in s.12 of the *CSIS Act* and not the reference to the analysis and retention of information and intelligence. From a functional perspective, the primary invasion of privacy is the collection of the information in the first place. That said, 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 rigorous standard of strict necessity. Even with respect to new information obtained from confidential and foreign sources, it may be difficult in practice to separate collection and retention issues. For reasons of practical necessity, it may be necessary to destroy some material shortly after it was collected because it should not have been collected in the first place because its collection was not strictly necessary. After this initial period, however, properly collected information should be analysed and retained without reference to the strictly necessary standard.

Despite the above interpretation, it is undeniable that s.12 has caused a number of difficulties. This critical section is not drafted as clearly as it could have been with respect to the grammatical placement of the "strictly necessary" qualifier. Moreover the purposes that are to be served

by the phrase "strictly necessary" in protecting privacy and its relation to the statutory mandate of CSIS are not clear. Section 12 could be amended so that the requirement of strict necessity applies only to the collection of intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada. Once collected information is determined to satisfy the statutory requirement that its collection was "strictly necessary", it should then be retained and subject to analysis as required to allow CSIS to conduct its lawful duties. These lawful duties include the possible disclosure of CSIS information under s.19(2) (a) of the CSIS Act for criminal investigations and prosecutions. Such an amendment would clarify CSIS's obligations with respect to the retention of properly collected intelligence.

Another possibility is to make specific reference to the enhanced need to retain information in CSIS's counter-terrorism investigations. Although criminal prosecutions could arise out of CSIS investigations into espionage, sabotage or subversion[232], they are more likely to occur with respect to its terrorism investigations. It may become necessary for a CSIS counter-terrorism investigation quickly to be turned over to the police so that people can be arrested and prosecuted before they commit acts that could kill hundreds or thousands of people. Section 12 could be amended to specify that CSIS should retain information that may be relevant to the investigation or prosecution of a terrorism offence as defined in s.2 of the Criminal Code or a terrorist activity as defined in s.83.01 of the Criminal Code. A reference to terrorism offences would be broader than a reference to terrorist activities because it would include indictable offences committed for the benefit of, or at the direction of, or in association with a terrorist group even if the offence itself would not constitute a terrorist activity. Information that is retained by CSIS because of its relevance in terrorism investigations or prosecutions could be of use to either the state or the accused in subsequent criminal prosecutions.[233]

Such an amendment would make clear that CSIS's mandate includes the retention of information and possible evidence that is relevant to terrorism investigations and prosecutions provided that the information was properly collected because its collection was strictly necessary for CSIS to investigate activities that may on reasonable grounds be suspected of

---

232 This is implicitly recognized in the *Security Offences Act* R.S. 1985 c.S-7 which gives the RCMP and the Attorney General of Canada priority with respect to the investigation and prosecution of offences that also constitute a threat to the security of Canada as defined in the CSIS Act.

233 Hon Bob Rae *Lessons To Be Learned* (2005) at 15-17.

constituting threats to the security of Canada. This would be consistent with amendments to Britain's *Security Service Act* which have made it clear that one of the functions of MI5 is to assist law enforcement agencies in the prevention and detection of serious crime and that information collected by MI5 in the proper discharge of its duties can be "disclosed for the purpose of the prevention or detection of serious crime or for the purpose of any criminal proceeding".[234] A similar provision about disclosure of information for criminal proceedings is also contained in the mandate of Britain's foreign intelligence agency.[235] The emphasis in the British legislation is on disclosure of information properly obtained by intelligence agencies whereas in Canada, there seems to be a need to emphasize that CSIS should both retain and disclose information that could assist in preventing or prosecuting serious crimes.

Increased retention of information by CSIS presents some dangers to privacy. An important protection for privacy would be that the requirement to retain information would only apply to information that satisfied either at the time of its collection or immediately afterwards, the "strictly necessary" requirement in the present s.12 of the CSIS Act. The *Privacy Act*[236] would also provide additional protections, albeit subject to the ability to disclose information under its consistent use and law enforcement provisions.[237] In addition, CSIS's review agency, SIRC, as well as its Inspector General, could play an important role in ensuring that information retained by CSIS was retained for purposes related to its statutory mandate and that this information was not improperly distributed. Finally, the Office of the Privacy Commissioner may also audit and review even the exempt banks of data held by CSIS.[238] Retained information should generally be kept secret. If information that is retained by CSIS is shared with others, it should be screened for relevance, reliability and accuracy. Proper caveats to restrict its subsequent disclosure should be attached.[239] Retained information by CSIS could in appropriate cases be passed on to the police under s.19(2)(a) of the CSIS Act or could be

---

234 *Security Services Act*, 1989 s.2(2)

235 *Intelligence Services Act*, 1994 s.2(2).

236 R.S.C. 1985 c. P-21

237 Ibid s.8. For a discussion of these restrictions see Commission of Inquiry into the Activities of Canadian Officials in Relation to Maher Arar *Analysis and Recommendations* (2006) at 337-338.

238 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* (2006) at pp. 286, 433-436. For a discussion of other restraints on information sharing by CSIS see Stanley Cohen *Privacy, Crime and Terror* (Toronto: Lexis Nexus, 2005) at 408.

239 See generally Commission of Inquiry into the Activities of Canadian Officials in Relation to Maher Arar *Analysis and Recommendations* (2006) at 334-343 in the context of information sharing by the RCMP.

subject to a court order of disclosure as was the case in *R. v. Malik and Bagri*.

G) Admission of CSIS Information under Business Records Exceptions

Intelligence can often be based on hearsay in the sense that it will report what another person purportedly heard another person say. Courts have in recent years become more willing to admit hearsay in cases where the hearsay is necessary and reliable. One of many exceptions that can allow the admission of hearsay evidence is the business records exceptions. In some cases, CSIS information could be admitted as evidence pursuant to s.30 of the *Canada Evidence Act*. That section contemplates the admissibility of records made "in the usual and ordinary course of business" with business defined to include "any activity or operation carried on or performed in Canada or elsewhere by any government…". This provision has been interpreted to allow evidence that would otherwise be hearsay. One restriction in s.30(10) of the Act provides that nothing in the section renders admissible "a record made in the course of an investigation or inquiry". This exception has been held to cover notes and logs of police investigations[240], as well as computer printouts from military equipment used to assist law enforcement officials in surveillance. It can be argued that investigations are important matters and that those conducting the investigation should have to testify and be subject to cross-examination. In the latter case, however, the records were admitted under the common law exception for business records made contemporaneously by a person under a duty to do so and with personal knowledge of the matters.[241]

Even if the restrictions in s.30(10) of the CEA were repealed and statutory or common law business records exceptions were used to introduce CSIS materials, CSIS officials could still likely be required to explain the significance of the material and the way it was obtained in order to explain why the material was reliable and why it was necessary to admit the material in a trial under the business records exception. This could require CSIS agents to testify to introduce the evidence. Steps could be taken to shield the identity of the CSIS employees from the public, but the accused would require sufficient information about the witnesses in order to be able to engage in meaningful cross-examination and challenges to credibility.

---

240 *R. v. Palma* (2000) 149 C.C.C.(3d) 169 (Ont.S.C.J.)
241 *R. v. Sunila* (1986) 26 C.C.C.(3d) 331 (N.S.S.C.) applying *Ares v. Venner* [1970] S.C.R. 608.

H) Intelligence Collected Outside of Canada

The nature of international terrorism, including the terrorism behind the bombing of Air India Flight 182, suggests that a person identified by Canadian officials as a terrorist suspect may move between Canada and other countries. When a suspect moves away from Canada, Canadian officials may ask foreign officials to engage in surveillance of that person. Such international co-operation may be valuable, but there are dangers that a Canadian suspect may not necessarily be a high priority for a foreign agency or that a foreign agency might in some circumstances use methods that would be objectionable to Canadians and Canadian courts. There appears to be a gap in Canada's intelligence gathering capacities with respect to individual suspects who leave Canada. It appears not to be possible to obtain a warrant under the CSIS act in such circumstances. In turn, the activities of Canada's signals intelligence agency, the Communications Security Establishment (CSE) are restricted and may not be admissible because they are only subject to Ministerial as opposed to judicial authorization.

1) CSIS Wiretaps Directed at Activities Outside Canada

A recently released decision has concluded that the CSIS wiretap warrant scheme in s.21 of the *CSIS Act* cannot be used to obtain warrants to engage in electronic surveillance of Canadian targets outside of Canada. Blanchard J. of the Federal Court Trial Division found that s.21 of the *CSIS Act* did not clearly authorize the granting of warrants for CSIS to conduct electronic surveillance outside Canada. The case involved ten people who were subject to warrants under s.21 of the *CSIS Act*, but who apparently left Canada for an unnamed foreign country. All but one of the suspects were Canadian citizens, permanent residents or refugees.

Blanchard J. found that neither s.12 or s.21 of the *CSIS Act* specifically addressed the issue of whether CSIS powers would apply outside of Canada and, as such, failed to establish a clear legislative intent to violate principles of international law, such as "sovereign equality, non-intervention and territoriality", which would be violated should Canadian officials conduct electronic surveillance in a foreign country.[242] The result of this decision is that CSIS appears unable to obtain a warrant to conduct electronic surveillance abroad.

---

242 *Dans l'affaire d'une demande de mandates* Oct. 22, 2007. SCRS 10-07 at para 54.

The judgment also suggests that such extra-territorial activities will not violate s.8 of the Charter or any provision of the Criminal Code, nor necessarily CSIS's mandate to collect security intelligence relating to threats to the security of Canada.[243] If the decision is interpreted, however, to preclude the use of CSIS intercepts abroad, this may make Canada reliant on the conduct of such activities by foreign agencies or by Canada's signals intelligence agency, the CSE. As will be seen, the CSE regime has restrictions designed to protect the privacy of Canadians and it operates through a Ministerial authorization scheme that may make it more difficult to introduce the intelligence so obtained as evidence compared to the judicial authorization scheme of s.21 of the *CSIS Act*.

2) Intelligence Collected by CSE pursuant to Ministerial Authorization

Section 273.65(1) of the *National Defence Act,* which was amended as part of the 2001 *Anti-Terrorism Act,* provides that the Minister of Defence "may, for the sole purpose of obtaining foreign intelligence, authorize the Communications Security Establishment in writing to intercept private communications in relation to an activity or class of activities specified in the authorization." Section 273.65(2) provides:

> 2) The Minister may only issue an authorization under subsection (1) if satisfied that
>
> (a) the interception will be directed at foreign entities located outside Canada;
>
> (b) the information to be obtained could not reasonably be obtained by other means;
>
> (c) the expected foreign intelligence value of the information that would be derived from the interception justifies it; and
>
> (d) satisfactory measures are in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security.

---

243 Ibid at paras 62-63.

The above provision could authorize the invasion of privacy of Canadians who are at one end of a foreign conversation that is targeted by the Ministerial authorization. As with the constitutionality of s.21 of the *CSIS Act*, much will depend on whether the courts accept an exception from *Hunter v. Southam* standards for national security matters. Section 273.65 of the *NDA* is more vulnerable to Charter challenge than s.21 of the *CSIS Act* because there is no judicial authorization. At the same time, however, s.273.65 does have a variety of restraints, including the requirements of investigative necessity, foreign intelligence value and requirements for conditions to protect the privacy of Canadians. In addition, Canada's main allies in the collection of signals intelligence generally rely on Ministerial as opposed to judicial authorizations.[244] Finally, it is possible that the courts could read in any requirements to protect privacy that it found wanting under the section.[245]

The Special Senate Committee reviewing the Anti-Terrorism Act was told that no more than 20 Ministerial authorizations had been issued under the Act and that as of April, 2005 only five were active. The Arar Commission reported that as of March, 2006 only four ministerial authorizations were active under the foreign intelligence mandate of the CSE. [246] Given the small number of these authorizations and depending on their precise ambit, it is possible that a court might find, on the facts of a particular case, that investigators had indeed "crossed the Rubicon" and were focused on collecting information to determine the criminal liability of an individual.

The Special Senate Committee that reviewed the *Anti-Terrorism Act* rejected arguments for judicial authorization on the basis that warrants under present Canadian law do not have extra-territorial effect. Such laws could, however, be amended to provide for such authorization. Judicial authorization for extra-territorial surveillance of a suspect whether conducted by the CSE or CSIS would maximize the chances that courts would accept such intercepts as evidence.

The Special Senate Committee recommended that CSE have specific and public "information retention and disposal policies" in order to protect

---

244 Stanley Cohen *Privacy, Crime and Terror* supra at 231.

245 Ibid at 236

246 Commission of Inquiry into the Activities of Canadian Officials in Relation to Maher Arar *A New Review Mechanism for the RCMP's National Security Activities* at 144.

the privacy of Canadians. [247] Section 275.65(2)(d) already contains a restrictive standard that private communications only be retained if they "are essential to international affairs, defence or security." Although well intentioned, information disposal programmes should also accommodate the possibility that information obtained by the CSE could subsequently become relevant to a criminal investigation of an act of terrorism. Although any attempt to admit information obtained by the CSE pursuant to Ministerial authorization would be subject to vigourous Charter challenge by the accused, one of the lessons of the erasures of many of the CSIS wiretaps in the Air India case is the need to retain intelligence that may become relevant to criminal investigations either in Canada or abroad. The intelligence can become relevant because of its possible value to the prosecution or because of its possible value to the accused. It would be better for intelligence to be retained, and for the issues of the ultimate admissibility of that evidence to be decided at a subsequent trial, than for the intelligence to be destroyed. Although the retention of intelligence can have negative effects on privacy, steps can be taken to minimize the danger to privacy by, for example, ensuring that access to the intelligence is limited. CSE, like CSIS, is also subject to self-initiated review, which should be able to detect any improper sharing of information.

The above observations relate to one of the main themes of this study, namely the need for the practices of intelligence agencies to catch up to the current emphasis on terrorism as a prime threat to national security and to new crimes of terrorism. One of the relevant features of the new crimes of terrorism in the *Anti-Terrorism Act* is the fact that Canada has asserted jurisdiction to prosecute crimes of terrorism committed outside of Canada. Given the threat and nature of international terrorism, this approach may make eminent sense, but at the same time it may require rethinking of the CSE Ministerial authorization regime. One option would be to allow for CSE to obtain judicial authorization. Another option would be to amend the *CSIS Act* to make clear that CSIS, perhaps with the CSE's assistance[248], can conduct electronic surveillance abroad subject to Canadian judicial authorization and the consent of the foreign country. Both approaches would increase the likelihood that intelligence collected abroad could be admitted as evidence in a Canadian court.

---

247 Special Senate Committee *Fundamental Justice in Extraordinary Times: Main Report of the Special Senate Committee on the Anti-Terrorism* Act Feb. 2007 at 78-79, Recommendation 19.

248 Section 273.64 authorizes the CSE to assist police and intelligence agencies but subject to limitations imposed on those agencies, In *Dans l'affaire d'une demande de mandates* Oct. 22, 2007. SCRS 10-07 at para 70, Blanchard J. indicated in obiter that he found the arguments by CSIS, that it could be assisted by the CSE in conducting electronic surveillance abroad, to be persuasive.

A judicial warrant to authorize either CSIS or CSE to conduct electronic surveillance outside of Canada would not ensure that the intelligence would be admitted in a subsequent trial. The accused would be free to argue that the evidence was obtained in violation of the Charter and should be excluded under s.24(2) of the Charter. Nevertheless, a judicial warrant might be a valuable first step to the ultimate admissibility of intelligence in a criminal trial. The use of warrants could allow the state to argue that, even if intelligence obtained outside of Canada was obtained in violation of s.8 of the Charter, its admission in a terrorism trial would not bring the administration of justice into disrepute under s.24(2) of the Charter.

3) The Admissibility of Foreign Signals Intelligence

The Arar Commission reported that CSE may at times request information from its foreign intelligence partners at the requests of the RCMP and that "if the intelligence generated from these sources relates to the RCMP mandate, the CSE may share it with the RCMP."[249] Information obtained by foreign agencies, even acting in co-operation with Canadian officials, would not in themselves be subject to Charter standards. [250] At the same time, an accused in a Canadian trial could argue that the admissibility of such evidence would constitute an abuse of process or violate Charter rights.

Canadian courts might admit foreign intercepts if officials from a foreign agency were prepared to testify as to the manner in which the information was obtained. The actions of the foreign officials would not be subject to the Charter. There might, however, be Charter violations and admissibility problems if there was some evidence that Canadian officials had perpetrated some abuse, such as deliberate circumvention of Canadian laws by reliance on foreign officials. Courts might be more likely to make such findings in circumstances in which Canadian officials had "crossed the Rubicon" and focused on the criminal activities of specific individuals. Courts would also be concerned if it was established that request to foreign partners had been made to avoid Canadian laws restricting the use of electronic surveillance in Canada. In such cases, a warrantless foreign intercept might be effectively substituted for what should have been a Criminal Code authorization for electronic surveillance. On the

---

249 Commission of Inquiry into the Activities of Canadian Officials in Relation to Maher Arar *A New Review Mechanism for the RCMP's National Security Activities* at 145.

250 *R. v. Harrer*, [1995] 3 S.C.R. 562; *R. v. Terry*, [1996] 2 S.C.R. 207.

other hand, evidence obtained from foreign signals intelligence that was not tasked and targeted in such a manner might well be admissible in Canadian criminal trials because the evidence itself would be reliable and the foreign agency that obtained it would not be subject to the Charter. As a result of a recent Supreme Court decision, the same might be said about intelligence collected by Canadian officials acting outside Canada because the Charter appears no longer to apply to such activities. [251]

I) Summary

In complex international terrorism investigations there may be overlapping electronic surveillance by CSIS, the CSE, foreign intelligence agencies and the police as targets frequently move between Canada and foreign states. The Arar Commission has recently recognized that suspects may be transferred to and from CSIS and the RCMP depending on whether there is sufficient evidence to justify a criminal investigation or a security intelligence investigation. The Atwal case study, as well as the facts of the Bagri and Malik prosecution, suggests, that in some cases electronic surveillance obtained under a CSIS warrant may be sought to be admitted into a criminal trial. Although it is 20 years old, the Federal Court of Appeal's decision in *Atwal* is still the leading precedent holding the CSIS warrant scheme to be constitutional. Such a conclusion would require courts to accept the distinct purpose of intelligence gathering, as opposed to law enforcement, either when interpreting s.8 of the Charter or in considering whether a departure from *Hunter v. Southam* standards can be justified under s.1 of the Charter. Courts may be more inclined to find a Charter violation if they are persuaded that CSIS "crossed the Rubicon" by focusing on the penal liability of specific individuals. Even then, however, evidence obtained through a CSIS warrant might still be admitted under s.24(2) of the Charter.

Care should be taken in relying on the admissibility of CSIS intercepts in criminal trials, especially in terrorism investigations where there is a focus on specific individuals and there may be reasonable grounds to believe that a crime, including the many new crimes of preparation and support for terrorism, has been committed. One of the main themes of this study is that security intelligence agencies need to be aware of the possibility of prosecutions arising from their anti-terrorism work and the disclosure and evidentiary implications of such prosecutions. In all cases in which

---

251 *R. v. Hape* 2007 SCC 26.

CSIS obtains an electronic surveillance warrant in a counter-terrorism investigation, it should carefully consider whether there would be grounds for a Part VI Criminal Code warrant and whether the latter would be preferable. Such a process will require close co-operation between CSIS and the relevant police forces.

Given the enactment of many new terrorism offences, the elimination of the investigative necessity requirement and the extended one year time period available for Criminal Code wiretap warrants in terrorism investigations, it is not clear that Criminal Code warrants will always be much more difficult to obtain than CSIS warrants. Any extra effort spent in obtaining a Criminal Code warrant may pay off should there be a prosecution in which material obtained under the warrant is sought to be introduced. Use of the Criminal Code warrant will avoid litigation over whether the CSIS warrant scheme complies with the Charter. The Criminal Code regime also provides for editing of the material used to obtain the warrant before it is disclosed to the accused. One of the most important means of establishing a reliable and workable relation between intelligence and evidence in the counter-terrorism field is to constantly re-evaluate whether a prosecution may occur. Security intelligence agencies need to be aware of the possibility of a terrorism prosecution and the ensuing evidentiary and disclosure implications. The *Parmar* case also suggests that considerations about the protection of sources and witnesses cannot be ignored even during early stages of a terrorism investigation. It is possible that the *Parmar* case might have proceeded to trial had the informant consented to the disclosure to the accused of identifying information in the affidavit or if adequate means had been devised to allow full adversarial challenge to the warrant without disclosing information to the accused that would have identified the informant and potentially put that person's life at risk.

Suspects in international terrorism investigations may frequently move between Canada and foreign countries. A recent judicial decision has held that CSIS cannot obtain a warrant under s.21 of the *CSIS Act* to conduct electronic surveillance outside of Canada. Unless the *CSIS Act* is amended to clearly authorize extra-territorial surveillance, Canada may have to rely on surveillance conducted by foreign agencies and /or the use of CSE signals intelligence. There are problems with both options. Foreign agencies may not have the same priorities as Canadian agencies and they may employ methods that would not be used by Canadian agencies. The CSE relies upon Ministerial as opposed to judicial authorizations

and this may make it more difficult to have CSE intercepts admitted as evidence in court. CSE may also be even more reluctant than CSIS to go to court. Thought should be given to making it possible for Canadian security intelligence agencies to conduct electronic surveillance outside Canada, subject to judicial authorization and the consent of the foreign country where the surveillance will take place. This would keep in place the structure that governs the CSE, including the restrictions designed to ensure that the CSE only collects foreign intelligence and respects the privacy of Canadians.

The different mandates of security intelligence agencies and the police, as well as the different constitutional standards used to obtain information, have often been cited as a reason why intelligence cannot be used as evidence. In this section, we have seen that the CSIS warrant scheme has been upheld under the Charter and that intercepts obtained by CSIS, if retained, could possibly be introduced as evidence in terrorism prosecutions. Even if courts find that CSIS intercepts were obtained in violation of s.8, there would be a strong case, at least in the absence of deliberate circumvention of Criminal Code standards, inaccuracies in affidavits used to obtain the warrant, or reliance on clearly unconstitutional laws or warrants, that they should be admitted under s.24(2). The evidentiary use of intelligence comes with the price of disclosure to the accused and judicial requirements that information that is shielded from disclosure to the accused cannot be used to support the legality or constitutionality of the warrant. There is, however, a possibility that courts might accept that the use of a security-cleared special advocate with full access to all relevant information would be an adequate substitute for disclosure to the accused for the limited purpose of challenging the admissibility of evidence obtained under a warrant.

IV. Obligations to Disclose Intelligence

Even if the state does not attempt to use intelligence as evidence, the accused in terrorism prosecutions may request production and disclosure of intelligence. The broad definition of terrorism offences may make it difficult for the Crown to argue that intelligence about the accused or his or her associates is clearly not relevant and not subject to disclosure. Intelligence may also relate to the credibility of informants and other witnesses and to the methods that were used to investigate the accused.