The Unique Challenges of Terrorism Prosecutions:

Towards a Workable Relation Between Intelligence and Evidence

Kent Roach

The Unique Challenges of Terrorism Prosecutions

Kent Roach*

Introduction

This is a summary of a longer study[1] which examines the unique challenges presented by terrorism prosecutions arising from the relationship between intelligence and evidence as opposed to the common challenges presented by all complex and long criminal trials, especially those with multiple accused, multiple charges, multiple pre-trial motions and voluminous disclosure. The longer study contains detailed case studies of terrorism prosecutions in Canada. These studies suggest that Canada has had a difficult experience with terrorism prosecutions. Many of these difficulties can be related to problems in managing the relationship between security intelligence and evidence.

In some cases, the state will want to use intelligence in court because it constitutes the best evidence of a terrorist crime. There are barriers to the admissibility of intelligence as evidence in part because intelligence may have been obtained under standards that are less onerous for the state than would normally apply to police efforts to discover evidence. Attempts to use intelligence as evidence may require disclosure of other secret information. In any event, accused will often seek access to intelligence in order to defend themselves from terrorism charges. They may seek not only exculpatory evidence but also intelligence that is relevant to the credibility of witnesses or the process through which evidence was obtained. A failure to disclose relevant evidence and information to the accused can threaten the fairness of the trial and can lead to wrongful convictions of innocent people. There have been wrongful convictions in the past in terrorism cases in other countries that have been related to the absence of full disclosure.[2]

At the same time, the interests of justice are not served if the government is forced to disclose secret intelligence and information that is not necessary for the conduct of a fair trial. In such cases, the government will

---

* Professor of Law and Prichard and Wilson Chair in Law and Public Policy, University of Toronto. Opinions expressed in this executive summary are those of the author and do not necessarily represent those of the Commission or Commissioner. I thank Birinder Singh and Robert Fairchild for providing excellent research assistance.

1 Kent Roach *The Unique Challenges of Terrorism Prosecutions: Towards a Workable Relation Between Intelligence and Evidence* vol 4 of the Research Studies of the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182.

2 Bruce MacFarlane "Structural Aspects of Terrorist Trials" in this volume.; Kent Roach and Gary Trotter "Miscarriages of Justice in the War Against Terrorism" (2005) 109 Penn. State Law Review 1001.

be placed in the unnecessary position of choosing between disclosing information that should be kept secret to protect sources, investigations and foreign confidences or declining to bring terrorism prosecutions. Although this difficult choice of whether to disclose or dismiss[3] may be necessary in cases where a fair trial is not possible without disclosure, this choice should not be unnecessarily forced on the government.

Canada's Experience with Terrorism Prosecutions: The Case Studies

The choice between disclosure or failing to prosecute is not a matter of hypothetical theory. The longer study contains detailed case studies of terrorism prosecutions in Canada. In two prosecutions of alleged Sikh terrorists, the government essentially sacrificed criminal prosecutions rather than make full disclosure that would place informers at risk. One of these prosecutions involved Talwinder Singh Parmar widely believed to have been the mastermind of the bombing of Flight 182. The other involved a conspiracy to blow up another Air India plane in 1986.[4] Although the Air India trial of *R. v. Malik and Bagri* did go to verdict in 2005, it also could have collapsed over issues of whether secrets had to be disclosed had unprecedented steps not been taken to give the accused disclosure of secret material on conditional undertakings that the intelligence not be disclosed by the accuseds' lawyers to their clients.[5] In addition, the trial judge did not have to order a remedy for the destruction of intelligence including wiretaps and notes made by the Canadian Security Intelligence Service (CSIS) that he held should have been retained and disclosed to the accused only because he acquitted the accused.[6]

When the state attempts to introduce intelligence as evidence, it will have to make disclosure of some of the underlying information used to obtain the intelligence. Problems with affidavits used to obtain a CSIS wiretap lead to the collapse of a conspiracy to commit terrorism prosecution in *R. v. Atwal*.[7] In terrorism prosecutions, the accused may frequently seek disclosure of intelligence held by CSIS. The Federal Court can order that such intelligence should not be disclosed because of harms to national security, national defence or international relations under s.38 of the

---

3 Robert Chesney "The American Experience with Terrorism Prosecutions" in this volume.

4 *R. v. Parmar* (1987) 31 C.R.R. 256 and other related cases discussed in Part 3 of the full paper; *R. v. Khela* [1996] Q.J. no. 1940 and other related cases discussed in Part 5 of the full paper.

5 Robert Wright and Michael Code "The Air India Trial: Lessons Learned". See also Michael Code "Problems of Process in Litigating Privilege Claims" in A. Bryant et al eds. *Law Society of Upper Canada Special Lectures The Law of Evidence* (Toronto: Irwin Law, 2004).

6 *R. v. Malik and Bagri* 2005 BCSC 350

7 (1987) 36 C.C.C.(3d) 161 (Fed.C.A.) and other related cases discussed in the full paper.

Canada Evidence Act, but this requires separate litigation that may delay and fragment the prosecution. The *Kevork*[8] terrorism prosecution, the ongoing *Khawaja* [9] terrorism prosecution and the *Ribic*[10] hostage taking prosecution all reveal how the litigation of s.38 issues can delay and fragment prosecutions, although convictions were eventually obtained in both the *Kevork* and *Ribic* cases and the *Khawaja* trial is pending.

The Disclose or Dismiss Dilemma

Terrorism prosecutions may have to be abandoned unless the state is prepared to disclose information that is essential to a fair trial and unless there is a workable means to determine what information must be disclosed and what information can be protected from disclosure. Both intelligence agencies and the justice system need to adjust to the challenges presented by disclosure of intelligence in terrorism prosecutions. Intelligence agencies and the police can work on front-end strategies to make intelligence more usable in terrorism prosecutions. The courts and the legislature can work on back-end strategies that increase the efficiency and fairness of the process for protecting intelligence from disclosure and determining what intelligence must be disclosed to the accused.

Before the state is forced to abandon terrorism prosecutions in order to keep secrets or a trial judge is forced to stay proceedings as a result of a partial or non-disclosure order, the justice system should ensure that the secret information is truly necessary for a fair trial and that no other form of restricted disclosure will satisfy the demands of a fair trial. The public interest and the legitimate demands of the Charter will not be served by the unnecessary abandonment of criminal prosecutions in favour of preserving secrets that will not truly make a difference in the outcome or the fairness of the criminal trial. At the same time, the public interest and the legitimate demands of the Charter will not be served by unfair trials where information that should have been disclosed to or introduced by the accused is not available because of even legitimate concerns about national security confidentiality.

---

8 (1984) 17 C.C.C.(3d) 426 (F.C.T.D.) and other related cases discussed in the full paper

9 *Canada (AttorneyGeneral). v. Khawaja* 2007 FC 463; *Canada (Attorney General) v. Khawaja* 2007 FC 490; *Canada (Attorney General). v. Khawaja* 2007 FCA 342; *Canada (Attorney General) v. Khawaja* 2008 FC 560 discussed in Part 6 the full paper.

10 *Ribic v. Canada (Attorney General)* [2003] F.C.J. no. 1964 and other related cases discussed in Part 6 of the full paper

The search for reasonable alternatives that reconcile the demands of fairness and secrecy is not limited to the formal processes of justice system. Efforts must be made to convince confidential informants that their identity can be revealed through disclosure and testimony while at the same time preserving their safety through witness and source protection programs. Similarly, efforts must be made to persuade both domestic and foreign agencies to amend caveats that prohibit the use of their intelligence in court. The standard operating procedures of security intelligence agencies with respect to counter-terrorism investigations, including the use of warrants, the recording of surveillance and interviews and the treatment of confidential sources, should be reviewed in light of the disclosure and evidentiary demands of terrorism prosecutions. This does not mean that CSIS should become a police force.[11] It does, however, mean that CSIS should be aware of the evidentiary and disclosure demands of terrorism prosecutions. Reconciling the demands of fairness and secrecy is one of the most difficult tasks faced by the justice system. It is also one of the most important tasks if the criminal justice system is to be effectively deployed against terrorists.

Outline of the Paper

The first part of this paper will provide an introduction to the evolving distinction between intelligence and evidence. Although stark contrasts between secret intelligence and public evidence have frequently been drawn, the 1984 *CSIS Act* did not contemplate a wall between intelligence and evidence. The Air India bombing and 9/11 have underlined the need for intelligence to be passed on to the police and if necessary used as evidence. At the same time, intelligence agencies have legitimate concerns that this could result in the disclosure of secrets in open court and to the accused.

The second part of this paper will outline the major principles at play in the relationship between intelligence and evidence. They are 1) the need to keep legitimate secrets 2) the need to treat the accused fairly 3) the need to respect the presumption of open courts and 4) the need for an efficient process for terrorism prosecutions. Ultimately, there is a need to reconcile the need for secrecy with the need for disclosure.

---

11 For warnings about CSIS becoming a "stalking horse" or "proxy for law enforcement" see Stanley Cohen *Privacy, Crime and Terror Legal Rights and Security in a Time of Peril* (Toronto: LexisNexis, 2005) at 407.

Both secrecy and disclosure are very important. The disclosure of information that should be kept secret can result in harm to confidential informants, damage to Canada's relations with allies, and damage to information gathering and sharing that could be used to prevent lethal acts of terrorism. The non-disclosure of information can result in unfair trials and even wrongful convictions. Even if the disclosure of secret information is found to be essential to a fair trial, the Attorney General of Canada can prevent disclosure by issuing a certificate under s.38.13 of the *Canada Evidence Act* that blocks a court order of disclosure. The trial judge in turn can stay or stop the prosecution under s.38.14 if a fair trial is not possible because of non-disclosure.

Although most of the concern expressed about the relation between intelligence and evidence has been about keeping intelligence secret and protecting it from disclosure, there may be times when intelligence will be used as evidence in trial. This raises the issue of whether information collected by CSIS, including information from CSIS wiretaps, as well as CSE intercepts, can be introduced into evidence. Intelligence is generally collected under less demanding standards than evidence and this presents challenges when the state seeks to use intelligence as evidence. In addition the use of intelligence as evidence may require increased disclosure of how the intelligence was gathered. There are, however, provisions that allow public interests in non-disclosure to be protected, but these may affect the admissibility of evidence. These issues, including the appropriate balance between CSIS and Criminal Code warrants, will be examined in the third part of this paper.

The fourth part of this paper will examine disclosure requirements as they may be applied to intelligence. In *R. v. Malik and Bagri*, CSIS material was held to be subject to disclosure by the Crown under *Stinchcombe*. *Stinchcombe* creates a broad constitutional duty for the state to disclose relevant and non-privileged information to the accused. Even if in other cases CSIS is held not to be directly subject to *Stinchcombe* disclosure requirements, intelligence could be ordered produced to the judge and disclosed to the accused under the *O'Connor* procedure that applies to records held by third parties. A significant amount of intelligence could be the subject of production and disclosure in a terrorism prosecution.

The fifth part of this paper will examine possible legislative restrictions on disclosure through the enactment of new legislation to restrict *Stinchcombe* and *O'Connor* and through the expansion or creation

of evidentiary privileges that shield information from disclosure. The precedents for such restrictions on disclosure will be examined and attention will be paid to their consistency with the Charter rights of the accused including the important role of innocence at stake exceptions to even the most important privileges. Attention will also be paid to the effects of restrictions on disclosure on the efficiency of the trial process. Disclosure restrictions may generate litigation over the precise scope of the restriction or the privilege concerned, as well as Charter challenges.

The sixth part of this paper will examine existing means to secure non-disclosure orders to protect the secrecy of intelligence in particular prosecutions. This will involve the procedures contemplated for claiming public interest immunity and national security confidentiality under ss.37 and 38 of the *Canada Evidence Act*. Section 38, like other comparable legislation, is designed to allow for the efficient and flexible resolution of competing interests in disclosure and non-disclosure. It provides for a flexible array of alternatives to full disclosure including agreements between the Attorney General and the accused, selective redactions, the use of summaries, and various remedial orders including admissions and findings of facts, as well as stays of proceedings with respect to parts or all of the prosecution. A singular feature of s.38, however, is that it requires the litigation of national security confidentiality claims not in the criminal trial and appeal courts, but in the Federal Court. As will be seen, Canada's two-court approach differs from that taken in other countries. It requires a trial judge to be bound by a Federal court judge's ruling with respect to disclosure while also reserving the right of the trial judge to order appropriate remedies, including stays of proceedings, to protect the accused's right to a fair trial. It will be argued that the s.38 process can be made both fairer and more efficient by allowing the trial judge to see the secret intelligence and in appropriate cases to order that it not be disclosed to the accused. Throughout the trial the trial judge would retain the ability to re-assess whether disclosure is required for a fair trial.

The seventh part of this paper will examine the processes used in the United States, the United Kingdom and Australia to decide whether intelligence should be disclosed to the accused. In all these jurisdictions, unlike in Canada, the trial judge decides whether it is necessary to disclose intelligence to the accused. In Canada, this decision is made by a Federal Court judge with the trial judge then having to accept any non-disclosure order, but also having to decide whether a fair trial is possible in light of the non-disclosure order.

The conclusion of this paper will assess strategies for making the relationship between intelligence and evidence workable. Both front-end strategies that address the practice of intelligence agencies and the police and back-end strategies that address disclosure obligations and the role of courts are needed.

Some of the front-end strategies that could make intelligence more useable in terrorism prosecutions include 1) culture change within security intelligence agencies that would make them pay greater attention to evidentiary standards when collecting information in counter-terrorism investigations; 2) seeking permission from originating agencies under the third party rule for the disclosure of intelligence; 3) greater use of Criminal Code wiretaps as opposed to CSIS wiretaps in Canada and the use of judicially authorized CSIS intercepts as opposed to CSE intercepts when terrorist suspects are subject to electronic surveillance outside of Canada; and 4) greater use of effective source and witness protection programs.

Some of the back end strategies that could help protect intelligence from disclosure are 1) clarifying disclosure and production standards in relation to intelligence; 2) clarifying the scope of evidentiary privileges; 3) providing a means by which secret material used to support either a CSIS or a Criminal Code warrant can be used to support the warrant while subject to adversarial challenge by a security cleared special advocate; 4) providing for efficient means to allow defence counsel, perhaps with a security clearance and/or undertakings not to disclose, to inspect secret material; 5) focusing on the concrete harms of disclosure of secret information as opposed to dangers to the vague concepts of national security, national defence and international relations; 6) providing for a one court process to determine claims of national security confidentiality that allows a trial judge to re-assess whether disclosure is required throughout the trial; and 7) abolishing the ability to appeal decisions about national security confidentiality before a terrorism trial has started.

I. The Evolving Distinction Between Security Intelligence and Evidence

Stated in the abstract, the differences between intelligence and evidence are stark with the former aimed at informing governments about risks to national security and the latter aimed at prosecuting crimes in a public trial. At the same time, the relation between intelligence and

evidence is dynamic.[12] Crimes related to terrorism often revolve around behaviour that may also be the legitimate object of the collection of security intelligence. Even before the enactment of the *Anti-Terrorism Act* (ATA), terrorism prosecutions could involve allegations of conspiracies or agreements to commit crimes or other forms of preparation and support for terrorism. The *Anti-Terrorism Act* now criminalizes support, preparation and facilitation of terrorism and participation in a terrorist group. The preventive nature of anti-terrorism law narrows the gap between intelligence about risks to national security and evidence about crimes.

Intelligence can be kept secret if it is only used to inform government of threats to national security. There is, however, a need to reconcile secrecy with fairness in cases where the intelligence becomes relevant in an accused's trial. At times, the Crown may want to introduce intelligence into evidence because it may constitute some of the best evidence of a terrorism crime. In many other cases, the accused may demand disclosure of intelligence on the basis that it will provide evidence that will assist the defence.

1) The Distinction Between Intelligence and Evidence at the Time that CSIS Was Created

In 1983, a Special Senate Committee chaired by Michael Pitfield stressed the differences between law enforcement and security intelligence:

> Law enforcement is essentially reactive. While there is an element of information-gathering and prevention in law enforcement, on the whole it takes place after the commission of a distinct criminal offence. The protection of security relies less on reaction to events; it seeks advance warning of security threats, and is not necessarily concerned with breaches of the law. Considerable publicity accompanies and is an essential part of the enforcement of the law. Security intelligence work requires secrecy. Law enforcement is 'result-oriented', emphasizing apprehension and adjudication, and the players in the system- police, prosecutors, defence counsel, and the judiciary- operate

12 Clive Walker "Intelligence and Anti-Terrorism Legislation in the United Kingdom" (2005) 44 Crime, Law and Social Change 387; Fred Manget "Intelligence and the Criminal Law System" (2006) 17 Stanford Law and Public Policy Review 415.

> with a high degree of autonomy. Security intelligence is, in contrast, 'information-oriented'. Participants have a much less clearly defined role, and direction and control within a hierarchical structure are vital. Finally, law enforcement is a virtually 'closed' system with finite limits- commission, detection, apprehension, adjudication. Security intelligence operations are much more open-ended. The emphasis is on investigation, analysis, and the formulation of intelligence.[13]

The distinctions between intelligence and evidence collection could not have been stated more starkly. The proactive role of the police in preventing crime and prosecuting attempts and conspiracies to commit acts of terrorism were ignored. Not surprisingly, the possibility that intelligence could have evidential value in a criminal trial was also ignored. The above observations of the Pitfield Committee represented influential but flawed thinking about the distinction between law enforcement and intelligence at the time of the creation of CSIS and during the initial Air India investigation.

CSIS was created in 1984 with a mandate to investigate a broad range of threats to the security of Canada. Although these threats to the security of Canada included threats and acts of serious violence directed at persons or property for political ends within Canada or a foreign state, they also included espionage, clandestine foreign-influenced activities and the undermining by covert unlawful acts of the constitutionally established government of Canada. The *CSIS Act* was created during the Cold War, a context symbolized by reports that CSIS surveillance on Parmar was interrupted for surveillance of a visiting Soviet diplomat.[14]

The *CSIS Act* placed an emphasis on secrecy. It made it an offence to disclose information relating to a person "who is or was a confidential source of information or assistance to the Service" or Service employees "engaged in covert operational activities of the Service"[15]. At the same time, the *CSIS Act* did not contemplate absolute secrecy or that intelligence would never be passed on to law enforcement. Section 19(2) provided that

---

13 *Report of the Special Committee of the Senate on the Canadian Security Intelligence, Delicate Balance: A Security Intelligence Service in a Democratic Society* (Ottawa: Supply and Services Canada, 1983) at p.6 para 14.

14 Kim Bolan *Loss of Faith How the Air India Bombers Got Away with Murder* (Toronto: McClelland and Stewart, 2005) at 63.

15 *CSIS Act* s.18.

CSIS may disclose information to relevant police and prosecutors "where the information may be used in the investigation or prosecution of an alleged contravention of any law of Canada or a province…"[16]. Even in 1984, there was a recognition that CSIS could have intelligence that would be useful in both criminal investigations and prosecutions. The *CSIS Act* did not establish a wall between intelligence and relevant information that could be provided to the police. Its implicit understanding of the relation between the collection of intelligence and evidence was more complex and nuanced than the stark contrast articulated by the Pitfield committee.

The proactive role of the police in preventing and investigating crime in the national security area was also recognized in the *Security Offences Act*[17]. In that act, RCMP officers were given "the primary responsibility to perform the duties that are assigned to peace officers" in relation to offences that arise "out of conduct constituting a threat to the security of Canada" as defined in the *CSIS Act*. The duties of RCMP officers include the prevention of crime and the apprehension of offenders[18]. A broad range of offences including murder, attempted murder, other forms of violence or threatening behaviour, espionage, sabotage and treason could be involved in conduct that constitutes a threat to the security of Canada. In addition, the Criminal Code prohibits not only completed offences, but attempts beyond mere preparation to commit such offences, agreements or conspiracies between two or more people to commit offences and attempts to counsel, procure or instigate others to commit offences, as well as a broad range of assistance to criminal activity.

A close reading of the *CSIS Act* and the *Security Offences Act* suggests that the stark contrast that the Pitfield Committee made between reactive law enforcement and preventive intelligence gathering was simplistic. The foundational 1984 legislation contemplated the disclosure of intelligence to the police for use in criminal investigations and prosecutions. It established overlapping jurisdictions by giving CSIS a mandate to investigate threats of terrorism when such threats, both before and after completion, could constitute crimes that would be within the primary jurisdiction of the RCMP. The RCMP role was not solely reactive. They had a mandate to prevent crime and they could investigate and lay charges both before and after acts of terrorism.

---

16 Ibid s.19(2)(a).
17 R.S.C. 1985 c.S-7 s.6.
18 *RCMP Act* s.18

2) Disclosure Requirements and Tensions Between CSIS and the RCMP

In 1998 and 1999, SIRC conducted a study of RCMP/CSIS relations. It noted:

> At the root of the problems in the exchange of information between CSIS and the RCMP is the need for CSIS to protect information, the disclosure of which could reveal the identity of CSIS sources, expose its methods of operation or that could compromise ongoing CSIS investigations. On the other hand, some RCMP investigators see some CSIS information as evidence that is vital to a successful prosecution, but which can be denied to them by caveats placed on the information by CSIS or that even if used, will be subject to the Service invoking sections 37 and 38 of the Canada Evidence Act, an action that could seriously impede the RCMP's case. The Service view is that it does not collect evidence. This possible misunderstanding on the part of some RCMP investigators may result in certain CSIS information/intelligence being treated as though it were evidence but which might not stand up to Court scrutiny because it had not been collected to evidentiary standards. [19]

The SIRC report raised concerns that review of CSIS documents by the RCMP Air India task force "could potentially place an extensive amount of CSIS information at risk under the *Stinchcombe* ruling regardless of whether it was subsequently used as evidence."[20] This report turned out to be prescient as CSIS was found to be subject to *Stinchcombe* disclosure requirements at the Malik and Bagri trial.

SIRC noted that the concerns of both the RCMP and CSIS had been increased by the impact of the Supreme Court's 1991 decision in *Stinchcombe*. SIRC commented that:

> The impact of that decision is that all CSIS intelligence disclosures, regardless of whether they would be entered for evidentiary purposes by the Crown are subject to disclosure to the Courts. Any passage of information,

---

19 CSIS Co-operation with the RCMP Part 1 (SIRC Study 1998-04) 16 October, 1998 at 9.
20 ibid at 14-15.

> whether an oral disclosure or in a formal advisory letter, could expose CSIS investigations. This means that even information that is provided during joint discussions on investigations or that is provided as an investigative lead is at risk.[21]

Although *Stinchcombe* defined disclosure obligations broadly, it did not define them in an unlimited manner. Disclosure obligations were subject to qualifications based on relevance to the case, privilege, including police informer privilege, as well as with respect to the timing of disclosure. In addition, the Attorney General of Canada could assert public interest immunity to prevent disclosure. Indeed, this had already been successfully done in at least one terrorism prosecution. [22]

These reports affirmed that the traditional divide between intelligence and evidence was still present and that concerns about compromising intelligence had been significantly expanded as a result of *Stinchcombe*. Although SIRC may have overestimated some of the impact of *Stinchcombe*, it was clear that many within the RCMP and CSIS believed that *Stinchcombe* had aggravated the tensions arising from the different mandates of the two agencies.

3) The Post 9/11 Era

The need for sharing of information and the conversion of intelligence to evidence took on greater urgency after 9/11 In 2005, the Hon. Bob Rae stressed the need to establish a workable and reliable relationship between intelligence and evidence. He placed the relationship between intelligence and evidence into its larger political, historical and legal context by observing that:

> The splitting off of security intelligence functions from the RCMP, and the creation of the new agency, CSIS, came just at the time that terrorism was mounting as a source of international concern. At the time of the split, counter-intelligence (as opposed to counter-terrorism) took up 80% of the resources of CSIS. The Cold War was very much alive, and the world of counter-intelligence and counter-espionage in the period after 1945 had created a culture of

---

21 Ibid at 9

22 See the case study of the *Kevork* prosecution in Part 6 of the full paper.

> secrecy and only telling others on a "need to know" basis deeply pervaded the new agency.

He then went on to note some of the implications of 9/11:

> The 9/11 Commission Report in the United States is full of examples of the difficulties posed to effective counter-terrorist strategies by the persistence of "stovepipes and firewalls" between police and security officials. Agencies were notoriously reluctant to share information, and were not able to co-operate sufficiently to disrupt threats to national security. There is, unfortunately, little comfort in knowing that Canada has not been alone in its difficulties in this area. The issue to be faced here is whether anything was seriously wrong in the institutional relationship between CSIS and the RCMP, whether those issues have been correctly identified by both agencies, as well as the government, and whether the relationships today are such that we can say with confidence that our security and police operations can face any terrorist threats with a sense of confidence that co-operation and consultation are the order of the day.
>
> The intelligence-evidence debate is equally important. If an agency believes that its mission does not include law enforcement, it should hardly be surprising that its agents do not believe they are in the business of collecting evidence for use in a trial. But this misses the point that in an age where terrorism and its ancillary activities are clearly crimes, the surveillance of potentially violent behaviour may ultimately be connected to law enforcement. Similarly, police officers are inevitably implicated in the collecting of information and intelligence that relate to the commission of a violent crime in the furtherance of a terrorist objective.[23]

Rae commented that the failure to preserve CSIS tapes on Parmar could have harmed both the state's interest in crime control and the interest of the accused in due process. The tapes could have contained incriminating evidence that could be used in criminal prosecutions, but alternatively

---

23 Hon. Bob Rae *Lessons to be Learned* (2005) at 22-23.

they could have contained exculpatory evidence or other information of assistance to the accused. In any event, the destruction of the tapes, as well as CSIS interview notes, allowed the accused to argue that they were deprived of exculpatory evidence. Rae commented that:

> The erasure of the tapes is particularly problematic in light of the landmark decision of the Supreme Court of Canada in *R. v. Stinchcombe*, which held that the Crown has a responsibility to disclose all relevant evidence to the defence even if it has no plans to rely on such evidence at trial. Justice Josephson held that all remaining information in the possession of CSIS is subject to disclosure by the Crown in accordance with the standards set out in *Stinchcombe*. Accordingly, CSIS information should not have been withheld from the accused.[24]

The Rae report highlighted the need for further study of the relationship between evidence and intelligence in light of *Stinchcombe* and the new focus on counter-terrorism including the creation of many new crimes related to the preparation and support of terrorism.

4) Summary

The RCMP and CSIS retain and should respect their different mandates, but they operate in a dynamic legal and policy environment. The crime prevention and evidence collection mandate of the RCMP has increased with the enactment of the 2001 ATA providing many new terrorism offences. The RCMP has also recognized that terrorism investigations must be more centralized than other police investigations; that they must be informed by intelligence; and that they must involve more co-operation with a wide variety of other actors including CSIS.[25] Security intelligence agencies may more frequently possess information that could be useful in criminal investigations and prosecutions especially under the ATA.

The above developments suggest a need to re-think stark contrasts between reactive policing and proactive intelligence; between decentralized policing and centralized intelligence and between secret intelligence and public evidence. All of these contrasts are based on the

---

24 Ibid at 16.

25 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) ch.4.

conventional wisdom when CSIS was created in 1984 during the Cold War even though a close reading of the *CSIS Act* and the *Security Offences Act* suggests a recognition that intelligence may have to be passed onto to the police when relevant to a police investigation and prosecution. The 1985 Air India bombings producing 331 deaths should have shattered simplistic dichotomies between secret intelligence and public evidence. Nevertheless, they persisted for some time and played a role in tensions between the RCMP and CSIS. In any event, the events of 9/11, and the passage of the 2001 ATA, should result in a thorough re-evaluation of the relation between intelligence and evidence.

Intelligence about terrorism can be relevant to possible criminal investigations into a wide range of serious criminal offences involving various forms of support, association and participation in terrorism and terrorist groups. Many of these investigations focus on associations and activities of targets and persons of interest. Such intelligence can be valuable to accused persons when defending themselves against allegations of support for and participation in terrorism. Although the need to protect sources, methods, ongoing investigations and foreign intelligence remains important, these demands should be re-thought in light of the need to prosecute and punish terrorists. Security intelligence agencies may have to become better acquainted with witness protection programs that are used in the criminal justice system and the demands of the collection of evidence. In this respect, it is noteworthy that MI5 accepts the need to collect some evidence (albeit not concerning electronic surveillance which is still generally inadmissible in British

courts) to an evidentiary standard. .[26] Requests may have to be made to foreign agencies for their consent to the disclosure of some information for the purposes of criminal prosecutions. Foreign countries are also dealing with the demands of terrorism prosecutions and may be willing to consider reasonable requests to allow the disclosure of some intelligence that they have provided to Canada. The world has changed since the original creation of *CSIS Act*. There is a need for some new and creative thinking that challenges conventional wisdom in order to ensure a workable relationship between intelligence and evidence.

II. Fundamental Principles Concerning Intelligence and Evidence

There are four principles, all well grounded in law, that have to be reconciled in managing the relation between intelligence and evidence.

1) The Need to Keep Secrets

The disclosure of intelligence to the accused and the public can have serious adverse effects on ongoing investigations, security operations and ultimately to the ability of security agencies to help prevent acts of

---

26 Britain's domestic Security Service, better known as MI5, provides a relevant example of how a security intelligence service can adjust its activities to better accommodate the need for evidence that can be used against suspected terrorists. Its official web site contains a section entitled "evidence and disclosure" which explains "Security Service officers have been witnesses for the prosecution in a number of high profile criminal trials, and intelligence material has either been admitted in evidence or disclosed to the defence as "unused material" in a significant number of cases. This has occurred mostly in the context of our counter-terrorist and serious crime work. The increased involvement of the Service in criminal proceedings means that, when planning and carrying out intelligence investigations that may lead to a prosecution, we keep in mind the requirements of both the law of evidence and the duty of disclosure….where an investigation leads to a prosecution, prosecuting Counsel considers our records and advises which of them are disclosable to the defence. If disclosure would cause real damage to the public interest by, for example, compromising the identity of an agent or a sensitive investigative technique, the prosecutor may apply to the judge for authority to withhold the material. Such applications take the form of a claim for public interest immunity (PII)." MI5 "Evidence and Disclosure" at http://www.mi5.gov.uk/output/Page87.html (accessed Jan 21, 2007). The statutory mandate of MI5 contemplates the disclosure of information for the purpose of preventing or detecting serious crime and criminal proceedings and the co-ordination of its work with the police and other law enforcement agencies. *Security Services Act*, 1989 ss. 1.(4) 2(2).

terrorism. Disclosure of secrets could also expose a confidential source to harm, including torture or death. In both *Ruby*[27] and *Charkaoui* [28], the Supreme Court recognized the importance of the secrecy of the foreign intelligence that Canada receives from its allies and Canada's particular position as a net importer of intelligence. In addition both the 9/11 Commission and the Arar Commission have affirmed the importance of information sharing among and between governments. Such information sharing often depends on expectations that the information that is shared will be kept secret. Finally, the importance of protecting the identity of informers has been affirmed by the courts in a number of decisions.[29]

2) The Need to Treat the Accused Fairly

The need to treat the accused fairly and to ensure that there is a fair trial is the bedrock principle of fundamental justice. In *Charkaoui*[30], the Court made clear that while adjustments could be made because of the need to protect secrets and other national security concerns, at the end of the day any remaining procedure must be fundamentally fair. The Supreme Court in *R. v. Stinchcombe*[31] grounded the broad constitutional right of disclosure in the accused's right to full answer and defence and a concern with preventing miscarriages of justice. Even with respect to the production and disclosure of material held by third parties, the Court in *R. v. O'Connor*[32] stressed the importance of the accused's right to full answer and defence. Even the most zealously guarded privileges such as the police informer privilege are subject to an innocence at stake exception which can require disclosure to the accused in cases where an informer becomes a material witness or a participant.[33]

3) Respect for the Presumption of Open Courts

The presumption of an open court has long been recognized in Canadian law and was given renewed vigour by the Charter guarantee of freedom of expression. The open court presumption is not absolute and it does not apply to information protected by informer privilege. [34] More generally, limitations on the open court principle can be justified on a case-by-case basis as a proportionate restriction on freedom of expression. [35]

27 [2002] 4 S.C.R. 3.
28 2007 SCC 9.
29 *R. v. Leipert* [1997] 1 S.C.R. 287; *Named Person v. Vancouver Sun* 2007 SCC 43
30 2007 SCC 9
31 [1991] 3 S.C.R. 326
32 [1995] 4 S.C.R. 401
33 *R. v. Scott* [1990] 3 S.C.R. 979 at 996; *Named Person v. Vancouver Sun* 2007 SCC 43 at para 29.
34 *Named Person v. Vancouver Sun* 2007 SCC 43
35 *Re Vancouver Sun* [2004] 2 S.C.R. 332,

4) The Need for Efficient Court Processes

Few would dispute that punishment and incapacitation is the appropriate response for those who would prepare and plan to commit acts of terrorist violence and those who have committed such violence. Criminal trials can serve a valuable purpose in denouncing acts of terrorism and educating the public about the dangers of terrorism. They demonstrate a commitment to fairness and principles of individual responsibility in which only the guilty are punished, a quality that is the antithesis and the moral superior to terrorism which is designed to harm innocent people. Various international instruments including conventions in relation to terrorism also obligate Canada to treat and prosecute terrorism as a serious crime. Finally, the accused has a right to a trial within a reasonable time, a right that has social benefits as well as protections for the accused.[36]

5) Summary

The demands for an efficient, 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 would 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: The Implications of the Different Standards for the Collection of Security Intelligence and 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

36 *R. v. Morin* [1992] 1 S.C.R. 771.

crimes created in 2001. There are several barriers to using intelligence as evidence in terrorism prosecution. 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 to arrest and prosecute. 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.

1) The Admission of Electronic Surveillance Obtained by CSIS

One of the case studies that raises the above issue is *R. v. Atwal*.[37] In that case, the Federal Court of Appeal held that the CSIS wiretap warrant scheme did not violate the right against unreasonable searches and seizures under the Charter, but that the affidavit used to obtain the warrant would have to be disclosed to the accused subject to editing and national security confidentiality claims. Inaccuracies discovered in the disclosed affidavit led to the resignation of the first director of CSIS. CSIS, like its peer agencies such as MI5, must be prepared for the possibility that intelligence gathered in its terrorism investigations may in some cases be used as evidence or disclosed to the accused.

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 criminal law 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) 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

---

37 *R v. Atwal* (1987) 36 C.C.C.(3d) 161 (Fed.C.A.)

to allow the accused to challenge the warrant as part of the right to make full answer and defence. Disclosure is not absolute. The affidavit used to obtain the warrant can be edited to protect confidential sources and covert agents as required by s.18 of the *CSIS Act* . Material that is edited out of the affidavit could not be used to support the affidavit and in some cases this might result in the affidavit as edited being found insufficient to support the warrant. It is also possible for the Attorney General of Canada to make national security confidentiality claims to prevent disclosure of the affidavit.[38] Again, material that was subject to a non-disclosure order could not be used to support the warrant if challenged by the accused at trial.

2) The Admission of Electronic Surveillance Obtained under the Criminal Code

Although evidence obtained under a CSIS warrant can perhaps be admitted as evidence in a criminal trial, it may be better when possible to obtain a Criminal Code warrant. Such a conclusion, of course, assumes that there will be co-operation between the RCMP and CSIS in their terrorism investigations. The ATA has made Criminal Code electronic surveillance warrants more attractive from the state's perspective because now, like CSIS wiretap warrants, they can be issued for up to a year. [39] Unlike CSIS warrants[40], there is no longer a requirement of establishing that other investigative processes, including surveillance, informers, undercover agents and regular search warrants, would not be successful.[41] Although warrants under s.21 of the *CSIS Act* are granted when there are reasonable grounds to believe that a warrant is required to enable CSIS to investigate a threat to the security of Canada, Criminal Code warrants can now be granted on reasonable grounds related to a wide variety of terrorism offences, including financing of terrorism, participation in a terrorist group and the facilitation of terrorism.

The use of Criminal Code authorizations is, of course, not a panacea. Those warrants themselves will be challenged. The *Parmar* case study in the full paper underlines difficulties that may follow from disclosure of information used to obtain Criminal Code warrants. In that case, the prosecution collapsed because the warrant could not be sustained

---

38 ibid at 186.
39 Criminal Code s.186.1
40 CSIS Act s.21(5). CSIS warrants in relation to subversion under s.2(d) of the Act are limited to 60 days.
41 Criminal Code s.186 (1.1).

without disclosing the identity of an informant and the informant refused to go into witness protection. It is hoped that both warrant practice and witness protection have improved since that time. In any event, if *Parmar* was being decided today, it would be possible to argue that the wiretap evidence should be admitted under s.24(2) of the Charter even if the warrant was unconstitutional after the reference to the confidential informant or other intelligence gathering techniques was edited out.[42]

The Criminal Code now contemplates that the prosecutor can delete from the affidavit any material that the prosecutor believes would be prejudicial to the public interest including information that would compromise the identity of any confidential informant or ongoing investigations, prejudice the interests of innocent persons or prejudice future investigations by endangering "persons engaged in particular intelligence-gathering techniques."[43] There may, however, be a case for expanding s.187(4)(c) which seems to protect intelligence gathering only where disclosure would endanger the person engaged in the technique. Intelligence gathering techniques may have to be protected even when disclosure would not endanger those who collect the intelligence.

There is a price that is paid for editing out material in the affidavit and protecting it from disclosure. Material that is edited out cannot be used to support the validity of the warrant though it may be possible for an edited summary to provide the accused with sufficient information to be able to challenge the warrant. A trial judge can order the subsequent disclosure of deleted material only if it is required by the accused to make full answer and defence and a provision of a judicial summary would not be sufficient.[44] The Courts have recognized that full disclosure should be the rule and that cross-examination on the affidavits may be necessary in order to allow the accused to challenge the warrant.[45]

3) The Shifting Balance Between CSIS and Criminal Code Electronic Surveillance Warrants

In complex international terrorism investigations there may be overlapping electronic surveillance by CSIS, the CSE, foreign intelligence

---

42 At the time that *Parmar* was decided, an automatic statutory exclusionary rule applied to electronic surveillance obtained without a valid warrant. See case study in Part 3 of the full study.

43 Criminal Code s.187(4).

44 Criminal Code s.187(7).

45 *R. v. Garofoli* [1990] 2 S.C.R. 1421 at 1461; *Dersch v. Canada (Attorney General)* [1990] 2 S.C.R. 1505; *R. v. Durette* [1994] 1 S.C.R. 469. See also *R. v. Parmar* (1987), 34 C.C.C. (3d) 260 at 273.

agencies and the police. 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 domains of intelligence and evidence collection are shifting because of the creation of new terrorism 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 counter-terrorism 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. This, of course, assumes full co-operation between CSIS and the police in terrorism investigations.

When intelligence is being collected, security intelligence agencies must ask themselves whether they have "crossed the Rubicon" into a predominant focus on criminal liability. If they have crossed this line, the courts may rule that a Criminal Code warrant should have been obtained.[46] If at all possible, the state should not rely on complex after the fact adjudications about whether a line has been crossed or the possibility that security intelligence obtained in violation of the Charter may nevertheless be found to be admissible in a criminal trial under s.24(2) of the Charter. Section 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 schemes if they have been found to violate the Charter.

In cases where there are sufficient grounds for a Criminal Code authorization, preference should be given to the collection of evidence under the Criminal Code as opposed to CSIS warrants. This will require a willingness of CSIS to allow the police to take the lead in the particular investigation. Intelligence that is used to obtain a CSIS or a Criminal Code warrant may have to be disclosed to allow the accused to challenge the warrant as part of the right to full answer and defence. The affidavit, however, will be edited before disclosure in order to protect broad public interests in non-disclosure. Information that is edited out cannot be used to support the warrant and the trial judge may order disclosure to the extent required by full answer and defence. The existing system generally allows a broad range of information to be protected from disclosure when a warrant is challenged, but at the price of the state not being able to rely

---

46 *R. v. Jarvis* [2002] 3 S.C.R. 708. See generally Stanley Cohen *Privacy, Crime and Terror* (Toronto: LexisNexus, 2005) at 399ff

on edited out and protected information in order to sustain the legality or constitutionally of a warrant.

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

An issue that arose in *R. v. Malik and Bagri* is whether CSIS should retain intelligence for possible disclosure at a criminal trial. The judge ruled that in the circumstances of the investigation, CSIS was subject to *Stinchcombe* disclosure obligations and CSIS had violated the duty to preserve *Stinchcombe* material by destroying wiretap evidence and notes of an interview with a key witness.[47] No remedy was ordered for these violations only because a remedy was unnecessary in light of the acquittals.

The judge's ruling in *Malik and Bagri* indicated that CSIS should have retained intelligence because it had to be disclosed. At the same time, CSIS is bound by s.12 of the *CSIS Act*. It 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.

The words "strictly necessary" qualify the reference in the section to investigation as opposed to the reference to the analysis and retention of information. If information is collected to the standard of what is strictly necessary respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada, it should be analysed and retained without limiting either analysis or retention to that which is strictly necessary. The collection of the information and intelligence should be limited to what is "strictly necessary" for reasons related to privacy, but the analysis of the collected information should not be so limited. Retention of information can, however, implicate privacy interests.

---

47 *R. v. Malik* [2002] B.C.J. No. 3219; *R. v. Malik* [2004] B.C.J. no. 842

Care should be taken to ensure that only information that when collected was "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 practically be difficult 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 including the possible disclosure of CSIS information under s.19(2) (a) of the CSIS Act for criminal investigations and prosecutions of crimes that also constitute threats to the security of Canada. 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[48], 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

48 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.

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.[49]

Such an amendment would make clear that CSIS's mandate includes the retention of information and 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 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".[50] A similar provision about disclosure of information for criminal proceedings is also contained in the mandate of Britain's foreign intelligence agency.[51] 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 detecting serious crime or for the purpose of criminal proceedings.

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*[52] would also provide additional protections, albeit subject

49 Hon Bob Rae *Lessons To Be Learned* (2005) at 15-17.
50 *Security Services Act*, 1989 s.2(2)
51 *Intelligence Services Act*, 1994 s.2(2).
52 R.S.C. 1985 c. P-21

to the ability to disclose information under its consistent use and law enforcement provisions.[53] 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.[54] 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.[55] 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 subject to a court order of disclosure as was the case in *R. v. Malik and Bagri*.

5) The Use of CSIS Material under the Business Records Exception

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 exception. Section 30 of the *Canada Evidence Act* (CEA) 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 the admission of evidence that would otherwise be hearsay. One restriction in s.30(10) of the Act which 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[56], as well as computer print outs from military equipment used to assist law enforcement officials in a surveillance. It can be argued that investigations are important matters and that those conducting the investigation should have to testify and

---

53 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.

54 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.

55 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.

56 *R. v. Palma* (2000) 149 C.C.C.(3d) 169 (Ont.S.C.J.)

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.[57]

Even if statutory or common law business records exceptions were used to introduce CSIS materials and the restrictions in s.30(10) of the CEA were repealed, CSIS officials could still 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. Use or expansion of the business records may not necessarily prevent CSIS agents from having to testify in criminal trials.

6) 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.

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 Canadians outside of Canada. Blanchard J. of the Federal Court Trial Division found that s.21 of the CSIS failed to establish a clear legislative intent to violate principles of international law such as "sovereign equality, non-intervention and territoriality" that would be violated should Canadian officials conduct electronic surveillance in a foreign country.[58] The result of this decision is that CSIS appears unable to obtain a warrant to conduct electronic surveillance abroad. At the same time, the judgment 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.[59]

---

57 *R. v. Sunila* (1986) 26 C.C.C.(3d) 331 (N.S.S.C.) applying *Ares v. Venner* [1970] S.C.R. 608.
58 Dans l'affaire d'une demande de mandates Oct. 22, 2007. SCRS 10-07 at para 54.
59 Ibid at paras 62-63.

One possible alternative is to allow Canada's signals intelligence agency, the CSE, to attempt to collect intelligence and intercept communications of a suspect outside of Canada. The CSE is, however, restricted to the collection of foreign intelligence and there is a requirement that there be satisfactory measures 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. [60]CSE intercepts are also authorized by the Minister of National Defence as opposed to a judge. The lack of prior judicial authorization will make intelligence gathered by the CSE more difficult to admit as evidence than electronic surveillance obtained by CSIS under a judicial warrant. It may be advisable to amend the CSIS Act to allow CSIS to obtain a judicial warrant to conduct electronic surveillance outside of Canada with the consent of the foreign country.

Another issue is whether a CSE or a foreign signals intelligence intercept might be used as evidence. Some might argue that it is fanciful to think that a signals intelligence intercept would ever be used in a terrorism prosecution, but such a view needs to be constantly re-evaluated in light of the nature of both international terrorism and communications. CSE intercepts will target foreign communications, but the *Anti-Terrorism Act* criminalizes various acts of terrorism outside of Canada. Another alternative to the possible use of CSE intercepts would be the use of intercepts obtained by foreign agencies. The current jurisprudence suggests that the Charter would not apply to the actions of foreign intelligence agencies even if they were acting in co-operation with Canadian officials and that it would not apply to Canadian actions abroad.[61] It is another matter whether a foreign country would consent to the use of its intelligence as evidence in a Canadian proceeding. Again the changing nature of international terrorism and communications suggests that it might be premature to conclude that signals intelligence would never be used as evidence in a terrorism prosecution.

7) Summary

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 CSIS obtains an electronic surveillance

60 *National Defence Act* s.273.65
61 *R. v. Hape* 2007 SCC 26.

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. Affidavits used to obtained either CSIS or Criminal Code wiretap warrants may have to be disclosed to the accused, but they can be edited to protect public interests in non-disclosure. In addition, the Attorney General of Canada can also make applications under s.38 of the CEA for non-disclosure of information that would injure national security, national defence or international relations. Material that is edited out of the affidavit, as in *Parmar*, cannot be used to sustain the warrant. Unlike in that case, however, the state retains the ability to seek admission of evidence obtained under an invalid warrant under s.24(2) of the Charter. The *Parmar* case also suggests that considerations about the protection of sources and witnesses cannot be ignored even during early stages of terrorism investigation because it is possible that the case might have proceeded to trial had the informant consented to the disclosure of information in the affidavit that would had the likely effect of identifying him or her.

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.

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 the Criminal Code or Charter standards, inaccuracies in affidavits used to obtain the warrant or persistent reliance on unconstitutional laws or practices, that intelligence obtained under

a CSIS electronic surveillance warrant should be admitted under s.24(2). The evidentiary use of intelligence will, however, come with the price of retention and disclosure of the intelligence. The requirement of disclosure is not, however, absolute and the affidavit used to obtain either a CSIS or a Criminal Code wiretap can be edited to protect various public interests in non-disclosure. In addition, the Attorney General of Canada retains the right to seek non-disclosure orders under s.38 of the CEA. Finally, there is 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.

1) Disclosure under *Stinchcombe*

The Supreme Court's 1991 decision in *Stinchcombe* [62]recognized a broad right to disclosure of relevant and non-privileged information. Although the right to disclosure is broad, the prosecutor need not disclose material that is clearly irrelevant to the case and of no use to the accused. [63] There are some signs that prosecutors may have overestimated the requirements of their *Stinchcombe* disclosure obligations in the ongoing *Khawaja* terrorism prosecution with respect to the need to disclose general analytical intelligence and internal administrative materials that could not be useful to the accused in his defence.[64]

On the particular facts of the Air India investigation, CSIS was held subject to *Stinchcombe* disclosure obligations including the duty to preserve

---

62 [1991] 3 S.C.R. 326

63 *R. v. Egger* [1993] 2 S.C.R. 451; *R. v. Chaplin* [1995] 1 S.C.R. 727.

64 *Canada v. Khawaja* 2007 FC 490 revd on other grounds 2007 FCA 342; *Canada v. Khawaja* 2008 F.C. 560. See discussion in Part 6 of the full study.

evidence. This holding would likely not be applicable to all CSIS activity, but it may be applied to some CSIS counter-terrorism investigations that focus on suspected individuals who may well be charged with terrorism offences or on information that CSIS shares with police who are investigating terrorism offences. Questions may arise in individual cases whether the Crown as prosecutor has control of intelligence material that may have formed the backdrop for a referral of an investigation from CSIS to the police or whether a CSIS investigation constitutes fruits of an investigation for the purposes of disclosure.[65]

Stinchcombe has been interpreted to require the preservation of evidence. CSIS's destruction of tapes and notes were held in *Malik and Bagri* to have violated this right.[66] Some might argue that the destruction of the tapes and interview notes was supported by the "strictly necessary" restriction in s.12 of the *CSIS Act*. As discussed above, the better view is that the requirement of strict necessity in that section applies to the collection of information and not its subsequent retention or analysis. Properly obtained information that may become relevant to a terrorism prosecution should be retained subject to safeguards to protect privacy and to ensure the lawfulness and review of any distribution of the information held by CSIS.

A violation of the right to disclosure under *Stinchcombe* does not necessarily violate the accused's right to full answer and defence. The courts on appeal have been willing to accept that violations of the broad right to disclosure of relevant information do not necessarily violate the right to full answer and defence or require a new trial. There are arguments that the right to disclosure exists in order to allow the accused to make full answer and defence and that the right to full answer and defence is more important than the right to disclosure. At the same time, courts in deciding whether the right to full answer and defence has been violated will be concerned about the cumulative effects of non-disclosure and whether there is reasonable possibility that non-disclosure would affect the outcome of the trial or the fairness of the process.[67]

---

65 See *R. v. Gingras* (1992) 71 C.C.C.(3d) 53 (Alta.C.A.) rejecting a request to a provincial prosecutor for disclosure of correctional records held by federal agencies. Higher standards of relevance can be imposed with respect to information that is not possessed or controlled by prosecutors as fruits of investigation or if there is a privacy interest in the material. *R. v. McNeil* (2006) 215 C.C.C.(3d) 22 (Ont.C.A.). See generally David Paciocco "Filling the Seam Between *Stinchcombe* and *O'Connor: The McNeil* Disclosure Application" (2007) 53 C.L.Q. 230.

66 *R. v. Malik* [2002] B.C.J. No. 3219; *R. v. Malik* [2004] B.C.J. no. 842

67 *R. v. La* [1997] 2 S.C.R. 680; *R. v. Dixon* [1998] 1 S.C.R. 244; *R. v. Taillefer* [2003] 3 S.C.R. 307.

2) Production and Disclosure of Third Party Records under *O'Connor*

Even if intelligence is found not subject to *Stinchcombe* disclosure requirements, CSIS and perhaps even CSE would be liable to demands for production of relevant information under the procedure contemplated for records possessed by third parties in *R. v. O'Connor*.[68] In such a case, the accused would first have to establish that the information sought to be obtained is likely to be relevant to an issue at trial or the competence of a witness to testify. This standard is higher than the *Stinchcombe* standard of relevance, but is not designed to be an onerous burden on an accused who is not engaged in a speculative or disruptive request for production.

Once the intelligence records were produced before the judge, the judge might balance a number of factors in deciding whether they should be disclosed to the accused. Whether this balancing would occur may depend on whether the judge found that the state's interest in non-disclosure of intelligence was as weighty as the privacy interests of complainants in sexual assault cases. The factors that might be included in the balance could include the extent to which access to the intelligence was necessary for the accused to make full answer and defence, its probative value in any trial and the prejudice that disclosure could cause to state interests and privacy or other rights. Even if CSIS was held not to be subject to *Stinchcombe*, it would be subject to the *O'Connor* process for obtaining the production and disclosure of third party records.

V. Methods of Restricting the Disclosure of Intelligence

There are a variety of means through which Parliament or the courts could place restrictions on the production and disclosure of intelligence. Parliament's legislation in response to *O'Connor* provides some precedent both for placing legislative restrictions on *Stinchcombe* and on the process for obtaining the production of third party records. Such legislation might attempt to create categories of intelligence that could not be disclosed or establish new procedures and new barriers for accused who seek the disclosure of intelligence. *Mills* suggests that legislative restrictions on disclosure may be held to be consistent with the Charter even if they result in the Crown having some relevant information that is not disclosed to the accused. It also suggests that Parliament can provide legislative

68 [1995] 4 S.C.R. 411.

guidance and procedures to govern production from third parties. Finally, *Stinchcombe* disclosure does not apply to information covered by evidentiary privileges such as police informer privileges. Such privileges could possibly be expanded by legislation.

All of these strategies to restrict the production and disclosure of intelligence would be subject to challenge as violating the accused's rights under the Charter. Even the strongest privileges are subject to innocence at stake exceptions. Restrictions on production and disclosure must still respect the accused's right to full answer and defence. Legislation that restricts the Charter also must survive a test of proportionality. Although various restrictions on *Stinchcombe* and *O'Connor* would be rationally connected to the protection of secrets and the effective operation of security intelligence agencies, it is not clear that they would be the least restrictive or best tailored means to protect secrets.

1) Legislation Limiting *Stinchcombe* and *O'Connor*

Legislation restricting Stinchcombe or O'Connor applications to obtain production and disclosure of intelligence could be defended as a reasonable limit on the accused's Charter rights to disclosure and to full answer and defence. The legislation would likely be rationally connected to the important objective of protecting secrets, but it could be argued that there are more proportionate alternatives for protecting secrets such as the existing provisions of ss.37 and 38 of the CEA that allow judges to assess the competing interests in disclosure and non-disclosure on the facts of particular cases. (These procedures will be discussed in Part VI below)

Legislative restrictions on disclosure or production would serve a similar purpose to s.38 proceedings in the Federal Court. If conducted by a trial judge, however, they might have some benefits in not requiring litigation in a separate court and the possibility of appeals before a trial starts. Allowing the trial judge to decide whether the information should be disclosed to the accused would follow the practice of other countries. It might also allow initial non-disclosure decisions to be re-visited in light of how the accused's interests in making full answer and defence evolve during the trial. In some cases, the state's interest in non-disclosure may change during the trial because of the lifting of caveats on information or the completion of investigations.

2) Expansion of Police Informer Privilege

Another possible means to restrict disclosure and production requirements of sensitive security information is to expand and codify privileges. The police informer privilege, for example, could be expanded to include CSIS informers or informers for other foreign security intelligence agencies. Some might even argue that CSIS itself should be treated as a police informer, even though the privilege has traditionally been designed to protect individuals and not entire state organizations from reprisals. The police informer privilege could also be expanded to apply in cases like *Khela* where the informer lost the benefits of the common law privilege by acting as an active agent. Matters covered by a valid privilege are not subject to the *Stinchcombe* disclosure requirement.

Such an expansion of privilege would not, however, be absolute. Although the courts zealously guard police informer privilege, they also have always recognized an innocence at stake exception to the privilege. The Supreme Court in *R. v. Scott*, recognized that "if the informer is a material witness to the crime then his or her identity must be revealed….. An exception should also be made where the informer has acted as agent provocateur".[69] This exception, as well as the need to reveal the identity of the informer in some search contexts, has recently been affirmed as valid examples of the innocence at stake exception.[70] This would seem to militate against the expansion of police informer privilege to apply to an informer like Billy Joe who acted as an agent in the Khela case.71 Even if an expanded police informer privilege was accepted, it would still be subject to an innocence at stake exception. It is more likely that innocence may be at stake when the informer is a material witness or an agent provocateur. Similarly, innocence would be more likely to be at stake if an entire organization such as CSIS was protected by an evidentiary privilege. Attempts to expand privileges beyond their natural limits could result in the privilege ultimately becoming a weaker, albeit broader, form of protection against disclosure.

3) Creation of a New National Security Class Privilege for Intelligence

Another possibility would be to create by legislation a new form of privilege such as a national security confidentiality privilege that would

---

69 *R. v. Scott* [1990] 3 S.C.R. 979
70 *Unnamed Person v. Vancouver Sun* 2007 SCC 43 at para 29.
71 *R. v. Khela* [1996] Q.J. no. 1940 discussed in part 6 in the full paper.

apply to CSIS material or some subset of CSIS material obtained from foreign agencies or to material that was shared between CSIS and the RCMP for co-ordination purposes. The Courts have often been reluctant to recognize new class claims of privilege. The Court has rejected a class privilege with respect to private records in sexual assault cases on the basis that such records can in some instances be relevant in criminal proceedings and that a class privilege would conflict with the accused's right to full answer and defence.[72] Similar concerns would apply to any new class privilege claim based on concerns about the harms to national security and international relations in disclosing intelligence. Some leading commentators doubt whether any new class privilege will be created and argue that "the self-interest of Ministers of government in asserting a class claim is evident and warrants close scrutiny."[73]

Any new national security privilege would have to be subject to the innocence at stake exception to be consistent with the Charter. If a new privilege was held to be less weighty than police informer or solicitor client privilege, it could also be subject to a broader exception to recognize the accused's right to full answer and defence. Both the innocence at stake and full answer and defence exceptions to privilege may be particularly broad in terrorism investigations. Terrorism investigations may involve far-reaching questions about the nature of the accused's associations with others within and outside of Canada. In addition, they may rely on human sources who may have been paid or protected by the state or who may be implicated in crimes. Some of this information might have to be disclosed even if a new privilege was created. It will simply not be possible to return to the pre-1982 days of an absolute privilege on broad national security grounds. Any new privilege to protect intelligence from disclosure would likely have to be created by statute and carefully tailored to apply to material whose disclosure would be particularly damaging. A class privilege would, however, have the advantage of providing the greatest amount of *ex ante* security that information covered by the privilege would not be disclosed. Even with respect to such a new class privilege, however, there would be an innocence at stake exception.

4) Case by Case Privilege to Protect Intelligence

A less drastic alternative to a new class privilege to shelter intelligence from disclosure would be a case by case privilege. It is possible that such

---

72 *A (L.B) v. B(A)* [1995] 4 S.C.R. 536

73 John Sopinka et al *The Law of Evidence* (Toronto: Butterworths, 1999) at 15.39.

a privilege might apply to information obtained by Canadian security intelligence agencies from foreign agencies and confidential sources on the basis that they constitute 1) communications originating in a confidence that they not be disclosed 2) confidentiality is essential to the full and satisfactory maintenance of the relation between the parties 3) the relation must be fostered and 4) the injury caused to the relation must be greater than the benefit of the correct disposal of the litigation.[74]

The privilege would again have to be reconciled with the accused's right to full answer and defence. Even in the private law context, the Court has rejected an all or nothing approach to privilege and held that disclosure of private records may be necessary in some cases.[75] In the context of private records in sexual assault cases, the Supreme Court also recognized that a case by case privilege approach would not address the main policy concerns about assuring complainants that their private records would never be disclosed.[76] A similar conclusion could be applied in the national security context. Even under a privilege approach, it would not be possible to assure foreign agencies, CSIS or CSIS informers that a disclosure order would never be made. [77]As will be seen, in the next section, the Attorney General of Canada already maintains the ability to issue a certificate under s.38(13) of the *Canada Evidence Act* (CEA) and/or to drop a prosecution in cases where a court has found disclosure of national security material to be necessary. Ultimately, this may be the only absolutely certain means to prevent the disclosure of intelligence.

5) Summary

The expansion of existing privileges such as the police informer privilege or the creation of a new privilege could possibly address problems with the extent of disclosure because *Stinchcombe* disclosure obligations do not apply to information protected by evidentiary privileges. Nevertheless, the certainty produced by such reforms in protecting intelligence from disclosure may be overestimated. Any new privilege will present its own threshold issues and there may be litigation about whether particular pieces of intelligence are covered by any privilege. Courts have been

---

74 8 Wigmore *Evidence* (McNaughton Rev. 1961) s 2285

75 *M (A) v. Ryan* [1997] 1 S.C.R. 157 at para 33. The Court stressed that the case for disclosure would be easier to make in a criminal case where the accused's liberty was at stake. Ibid at para 36.

76 *A (L.B) v. B(A)* [1995] 4 S.C.R. 536 at para 77.

77 The prohibition on the disclosure of confidential sources or covert agents of CSIS in s.18(1) of the CSIS Act is subject to s.18(2) which contemplates disclosure as required by law and for enforcement and prosecution reasons.

hesitant to recognize any new class privilege. The assertion of a case by case privilege will require litigation and will not afford certainty to CSIS, its foreign partners or CSIS informers that disclosure will never occur. It may be difficult to determine whether a case by case privilege applies without knowing the value of the information in the criminal trial. Even if a class privilege applies, all privileges must allow an innocence at stake exception. The determination of whether innocence or full answer and defence is at stake is a matter best decided by the trial judge.

Although a broadened police informer or state secrets privilege would be rationally connected to important objectives with respect to the keeping of secrets, it could be found to be a disproportionate restriction on the accused's Charter rights to disclosure and full answer and defence. The courts have refused to allow even the most established and cherished privileges to be absolute. Any privilege must be subject to at least an innocence at stake exception to be consistent with the Charter. Courts could also find that the existing regime under s.38 of the CEA, including the Attorney's General ability to block disclosure under s.38.13, constitute a less rights restrictive approach to the creation of new privilege. The section 38 procedure allows for a balancing of competing interests in disclosure and secrecy on the facts of the particular case.

Legislative restrictions on disclosure or production or any attempt to create new privileges are not a panacea to resolving the tensions between secret intelligence and evidence and other relevant information that must be disclosed in court. They would be vulnerable to Charter challenge. It is not clear whether *Mills* [78]is applicable in the national security context because the Court upheld restrictions on disclosure and third party production in that case on the basis that Parliament had reasonably reconciled the competing Charter rights of the accused and the complainant in sexual assault cases. It is not clear that terrorism cases would involve competing rights in the same manner as in *Mills*.

Even if legislation restricting disclosure or production or creating a new privilege was upheld under the Charter, there could be much litigation about the precise meaning of the legislation and its relation to Charter standards. Although the state's interests in non-disclosure are particularly strong in the national security context, there is also a particular danger that non-disclosure could increase the risk of miscarriages of justice in terrorism prosecutions. The non-disclosure of even apparently innocuous

78 [1999] 3 S.C.R. 668.

information about a suspected terrorist cell could deprive the accused of important resources to challenge the manner in which the state investigated the case and its failure to consider alternative understandings of ambiguous events and associations that could point in the direction of the innocence of the accused. Intelligence could also be relevant to the credibility of human sources and informants.

The courts will be concerned about the cumulative effects of non-disclosure when deciding whether restrictions on disclosure or production or a new statutory privilege violates the accused's right to full answer and defence.[79] Even if legislative restrictions on *Stinchcombe* or new and expanded privileges were upheld, they could require the judge to examine information sought to be exempted from disclosure item by item. This process would create uncertainty and delay. Although intended to decrease the need for the Attorney General of Canada to seek non-disclosure orders under s.38 of the CEA, legislative restrictions on disclosure or production or the attempt to create new privileges could add another layer of complexity, delay and adversarial challenge to terrorism prosecutions. They may duplicate and overlap with procedures already available under s.38 of the CEA to obtain non-disclosure orders. It may be better to reform the s.38 process to make it more efficient and more fair than to attempt to construct new and potentially unconstitutional restrictions on disclosure.

VI. Judicial Procedures To Obtain Non-Disclosure Orders

Although it is possible to attempt to lay out categorical restrictions on the disclosure of intelligence through legislative restrictions and the expansion and creation of privileges, it is also possible to obtain court orders under section 37 or 38 of the CEA that the public interest in non-disclosure outweighs the public interest in disclosure on the facts of a particular case. The *ex ante* legislative approach discussed in the last section may at first appear to provide greater certainty that intelligence will not be disclosed, but as suggested above, even the most robust privileges and legislative restrictions will be subject to some exceptions to ensure fair treatment of the accused. The techniques examined in this section are tailored to the facts of specific cases.

The procedures used to obtain non-disclosure orders vary considerably depending on the nature of the public interest in non-disclosure that is

79 *R. v. Taillefer* [2003] 3 S.C.R. 307.

asserted. Specified public interests in non-disclosure, as well as common law privileges, can be determined by superior court criminal trial judges under s.37 of the CEA. In contrast, national security confidentiality (NSC) claims under s.38 that the disclosure of information would injure national security, national defence or international relations must be determined by specially designated Federal Court judges. The trial judge must accept any non-disclosure order by the Federal Court, but also retains the right to order whatever remedy is required to ensure the fairness of the trial. A number of case studies in the longer paper, the *Kevork* and ongoing *Khawaja* terrorism prosecutions and the *Ribic* hostage-taking prosecution reveal how separate s.38 litigation can delay and fragment prosecutions. By requiring non-disclosure issues to be decided by two different courts, the Canadian approach runs the risks that intelligence might be disclosed when such disclosure is not necessary for a fair trial or that it might not be disclosed when it is necessary for a fair trial. As will be the seen, the Canadian approach has not been followed in other democracies.

1) Section 37 of the CEA and Specified Public Interest Immunity

Section 37 of the CEA provides a procedure for a Minister of the federal Crown or another official to apply to a court for an order that a specified public interest justifies non-disclosure or modified disclosure of certain material. Such applications can, in criminal matters, be heard by the superior court trial judge and be subject to appeal to the provincial Court of Appeal and the Supreme Court, but there is some precedent for allowing a trial to proceed, if possible, while these separate appeal rights are exercised.[80] . This procedure has been used in some cases to protect the identity of police informers and ongoing investigations.

Section 37 allows superior court trial judges in terrorism prosecutions, to make case-by-case decisions about disclosure. The judge determines whether the disclosure of the information would encroach upon the specified public interest. If so, the judge then determines whether the public interest in disclosure nevertheless outweighs the public interest that will be harmed by disclosure. The judge can place conditions on

---

80 *R. v. McCullogh* (2001) 151 C.C.C.(3d) 281 (Alta.C.A.); *R. v. Archer* (1989) 47 C.C.C.(3d) 567 (Alta.C.A.)

the disclosure including redactions and summaries to limit the harm of disclosure or requiring the prosecution to make an admission of fact as the price for non-disclosure of information.[81]

Section 37.3 also allows trial judges to fashion whatever appropriate and just remedy is required to protect the accused's right to a fair trial. Section 37.3 requires the trial judge, when fashioning such remedies, to comply with a non, or partial, disclosure order previously made under s.37. This raises the possibility that trial judges may be unable to revise their own previous non-disclosure orders under s.37, even if they conclude later in the proceedings that non-disclosure would adversely affect the right to a fair trial. As will be seen in the next section, judges in other countries have the ability to revise non-disclosure orders in light of developments during the trial. The ability of trial judges to revisit and revise non-disclosure orders builds an important flexibility into the system that can benefit both the accused and the prosecution. The accused could gain disclosure to information that appears necessary for a fair trial because of developments in the criminal trial. The prosecution retains the right to halt the prosecution in order to protect the information from disclosure.

2) Section 38 of the CEA and National Security Confidentiality

Section 38 of the CEA provides a complex procedure to govern the protection of information that if disclosed would harm national security, national defence or international relations. Unlike s.37 which allows superior court trial judges to make decisions, all non-disclosure claims under s.38 must be decided by the Federal Court. The trial judge must accept this decision, but can order any remedy that is necessary to protect the fairness of the trial as a result of the non-disclosure.

Justice system participants, including the accused, have obligations under s.38.01 to notify the Attorney General of Canada if they plan to disclose "information of a type that, if it were disclosed to the public, could injure international relations or national defence or national security" or "information relating to international relations or national

---

81 Section 37(5) provides: "If the court having jurisdiction to hear the application concludes that the disclosure of the information to which the objection was made under subsection (1) would encroach upon a specified public interest, but that the public interest in disclosure outweighs in importance the specified public interest, the court may, by order, after considering both the public interest in disclosure and the form of and conditions to disclosure that are most likely to limit any encroachment upon the specified public interest resulting from disclosure, authorize the disclosure, subject to any conditions that the court considers appropriate, of all of the information, a part or summary of the information, or a written admission of facts relating to the information."

defence or national security that is in the possession of the Government of Canada, whether originating from inside or outside Canada, and is of a type that the Government of Canada is taking measures to safeguard."[82] This notification requirement is designed to give the Attorney General advance notice and "to permit the government to take pro-active steps in the appropriate circumstances" and to minimize the need for "proceedings to come to a halt while the matter was transferred to the Federal Court for a determination."[83] Such a mid-trial invocation of s.38 is precisely what happened in the *Ribic* hostage taking trial, leading to the declaration of a mistrial. At the same time, however, "the scheme continues to permit the government to invoke the provisions of the CEA during the course of the hearing".[84] This means that s.38 issues could still arise during a criminal trial. For example, the Crown may make late disclosure accompanied by a s.38 claim. Another example is that the accused could, as in *Ribic*, propose to call a witness to testify about sensitive or potentially injurious information. Denying the accused the right to call a witness with relevant information could violate the accused's right to full answer and defence. As occurred in *Ribic*, extensive litigation might be necessary in the Federal Court during the middle of a criminal trial.

Under s.38.03, the Attorney General of Canada may "at any time and subject to any conditions that he or she considers appropriate, authorize the disclosure" of information which is prohibited from disclosure under s.38.02 because a notice has been given under s.38.01. Section 38.031 contemplates disclosure agreements among the Attorney General and persons who have given notice under s.38.01. If no disclosure agreement is made between the Attorney General and the accused, a hearing will take place before a specially designated judge of the Federal Court to determine whether there should be disclosure, modified or partial disclosure or non-disclosure of the material in dispute.

i. Ex Parte Submissions, Special Advocates and Non-Disclosure Undertakings with Defence Counsel

Both the Attorney General of Canada and the accused can make *ex parte* submissions to the judge. The accused's own lawyer can make *ex parte* submissions to the Federal Court. [85] The accused could reveal their

---

82 CEA s.38.01
83 Department of Justice Fact Sheet "Amendments to the Canada Evidence Act"
84 ibid
85 *Canada (Attorney General) v. Khawaja* 2007 FCA 342 at paras 34, 35.

planned defences to the Federal Court without disclosing them to the prosecutor or the trial judge. Defence counsel may, however, be reluctant or unable to do so at the pre-trial stage and without having seen the undisclosed information.

The ability of the Attorney General to make *ex parte* submissions has been upheld from Charter challenge, but with an indication that security cleared lawyers could, if necessary, be appointed to provide adversarial challenge. [86] The appointment of such lawyers would not be governed by a new law providing for special advocates in security certificate cases.[87] A security cleared lawyer will require time to become familiar with the case and this will likely cause further delay in s.38 proceedings. At the end of the day, the security cleared lawyer may never be as familiar with the case as the accused's own lawyer. Special advocates may play an important role in providing adversarial challenge to the government's claim of secrecy, but they will have more difficulty protecting the accused's right to full answer and defence given limitations on the security cleared lawyer's familiarity with the case and perhaps his or her ability to consult the accused and take instructions about the secret information. [88] The special advocate in a s.38 proceeding, however, would only be representing the accused's interest in full disclosure and challenging the government's claim for secrecy. The special advocate would not be attempting to challenge secret evidence as is the case under immigration law security certificates.

In *R. v. Malik and Bagri,* the accuseds' defence lawyers were able to examine undisclosed material on an initial undertaking that the information would not be disclosed to their clients. This allowed the lawyers most familiar with the case to determine the relevance and usefulness of the information and then to present focused and informed demands for disclosure.[89] The present alternative under s.38 is that defence lawyers must make broad and un-informed demands for disclosure because they have not seen the information.

---

86 *Canada (Attorney General) . v. Khawaja* 2007 FC 463 aff'd without reference to the ability to appoint security-cleared lawyers 2007 FCA 388.

87 *An act to amend the Immigration and Refugee Protection Act* S.C. 2008 c.3. But see *Khadr v. The Attorney General of Canada* 2008 FC 46 and *Canada (Attorney General) v. Khawaja* 2008 FC 560 appointing a security cleared lawyer to assist in s.38 proceedings.

88 Under the immigration law amendments governing special advocates, any consultation by the security cleared lawyer with others about the case after the security cleared lawyer has seen the information would have to be authorized by the judge.

89 Michael Code "Problems of Process in Litigating Privilege Claims" in A. Bryant et al eds. *Law Society of Upper Canada Special Lectures The Law of Evidence* (Toronto: Irwin Law, 2004).

ii. Reconciling the Interests in Secrecy and Disclosure

Under s.38.06, the Federal Court judge determines first whether the disputed information would be injurious to international relations, national defence or national security. If not, the information can be disclosed. If the information is injurious, the judge considers the public interest in both disclosure and non-disclosure. The judge also has the option of placing conditions on disclosure including authorizing the release of only a part or a summary of the information or a written admission of fact relating to the information. The emphasis under this section is on a flexible reconciliation of competing interests in disclosure and secrecy.[90] As such it accords with the approaches taken in other democracies.

Section 38(6) defines the harms of disclosure broadly as material whose disclosure "would be injurious to international relations or national defence or national security." The Senate Committee that reviewed the *Anti-Terrorism Act* recommended that the precise harms to international relations be enumerated more precisely. Such a harms based approach could also be applied to the vague terms of national security and national defence.[91] For example, section 38 could be amended to specify the harms of disclosure to vulnerable sources and informers, ongoing operations, secret methods of operation and with respect to undertakings given to foreign partners or at least to list such harms as examples of harms to national security, national defence or international relations. Such a harm based approach might help prevent the overclaiming of national security confidentiality. It might also help restore public confidence about the legitimate uses of secrecy.

---

90 Section 38(6) provides: "If the judge concludes that the disclosure of the information would be injurious to international relations or national defence or national security but that the public interest in disclosure outweighs in importance the public interest in non-disclosure, the judge may by order, after considering both the public interest in disclosure and the form of and conditions to disclosure that are most likely to limit any injury to international relations or national defence or national security resulting from disclosure, authorize the disclosure, subject to any conditions that the judge considers appropriate, of all of the information, a part or summary of the information, or a written admission of facts relating to the information."

91 In his s.38 decision with respect to the Arar Commission, Justice Noël attempted the difficult task of defining the operative terms of s.38. He suggested that national security the "means at minimum the preservation in Canada of the Canadian way of life, including the safeguarding of the security of persons, institutions and freedoms" *Canada v. Commission of Inquiry* 2007 FC 766 at para 68. National defence includes "all measures taken by a nation to protect itself against its enemies" and "a nation's military establishment". International relations "refers to information that if disclosed would be injurious to Canada's relations with foreign nations." Ibid at paras 61-62. The vagueness of the term national security is notorious. M.L. Friedland for example prefaced a study for the McDonald Commission with the following statement: "I start this study on the legal dimensions of national security with a confession: I do not know what national security means. But then, neither does the government." M.L. Friedland *National Security: The Legal Dimensions* (Ottawa: Supply and Services, 1980) at 1.

iii. Appeals under Section 38

The accused or the Attorney General has the ability under s.38.09 to appeal a decision made under s.38.06 to the Federal Court of Appeal. Although an appeal must be brought within 10 days of the order, there are no time limits on when the appeal must be heard or decided. The Federal Court of Appeal's decision is not necessarily final as the parties have 10 days after its judgment to seek leave to appeal to the Supreme Court. These provisions create a potential for national security confidentiality issues to be litigated all the way to the Supreme Court before a terrorism trial even starts or during the middle of a criminal trial.

iv. Attorney General Certificates under Section 38.13

The Attorney General of Canada can personally issue a certificate under s.38.13 to prohibit the disclosure of information ordered disclosed by the court. This certificate is subject to judicial review, but only to determine if the information was received from a foreign entity or relates to national security or national defence.

v. The Role of the Trial Judge under Section 38.14

Under s.38.14, the trial judge must respect any non or partial disclosure order made by the Federal Court under s.38.06 or an Attorney's General certificate under s.38.13. At the same time, the trial judge can also issue any order that he or she considers appropriate to protect the accused's right to a fair trial including a stay of proceedings on all or part of an indictment or finding against a party.

vi. Changing Approaches to National Security Confidentiality

Attitudes towards national security confidentiality have evolved considerably over the last 25 years. Until 1982, a federal Minister could assert an unreviewable claim to protect information on national security grounds. In the early 1980's, courts were reluctant even to examine material when national security was invoked.[92] There was considerable concern that the disclosure of even innocuous information could harm national security, national defence and international relations through the mosaic effect because of the abilities of Cold War adversaries to put

92 *Re Goguen* (1984) 10 C.C.C.(3d) 492 at 500 (Fed.C.A.).

together the pieces of information.[93] In recent years, however, courts have rightly been more skeptical about claims of the mosaic effect and have indicated that Canada should seek permission from allies to allow the disclosure of information under the third party rule.[94] Concerns have been raised that the overclaiming of national security confidentiality causes delays and creates cynicism about legitimate secrets.[95] The third party rule remains a critical component of legitimate claims of national security confidentiality, but it should not be invoked in a mechanical manner. It only applies to information that has been received in confidence from a third party and should not be stretched to apply to information that either was in the public domain or was independently possessed by Canadian agencies. Canadian agencies should also generally seek the consent of the originating agency to the use of information covered by the third party rule. Seeking amendments to caveats to request permission for further disclosure is perfectly permissible. It demonstrates Canada's respect for the caveat process and the third party rule.

vii. Summary

The 2006 RCMP/CSIS MOU contemplates the use of s.38 of the CEA as a means to protect intelligence passed from CSIS to the RCMP from disclosure in criminal and other proceedings. Nevertheless, s.38 imposes a time consuming and awkward process for reconciling the need for disclosure with the need for secrecy. It places obligations on justice system participants including the accused to notify the Attorney General of Canada about a broad range of sensitive and potentially injurious information. Section 38 applies to a very broad range of information that if disclosed would be injurious to international relations, national defence or national security. Thought should be given to narrowing the range of information covered by s.38 and to specifying the precise and concrete harms of disclosure of information. Providing specific examples of harms to national security and international relations could help discipline the process of claiming national security confidentiality and respond to the problem of overclaiming secrecy. In addition, it appears from both the *Ribic* and *Khawaja* prosecutions that prosecutors need to be reminded that they need not seek s.38 non-disclosure orders if the information is clearly irrelevant to the case and of no assistance to the accused.

---

93 *Henrie v. Canada* (1988) 53 D.L.R.(4th) 568 at 580, 578 affd 88 D.L.R.(4th) 575 (Fed.C.A.).

94 *Canada v. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar* 2007 FC 766; *Khawaja v. Canada* 2007 FC 490.

95 Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar *Report of the Events Relating to Maher Arar Analysis and Recommendations* (Ottawa: Public Works and Government Services) at pp 302, 304.

The ability of the Attorney General to make *ex parte* representations to the s.38 judge is only partly compensated for by the ability of the accused to make *ex parte* representations. The value of the accused's *ex parte* representations will be attenuated by the fact that the accused has not seen the secret information that is the subject of the dispute. Several decisions by the Federal Court Trial Division [96]have opened up the possibility of appointing a security cleared lawyer who, unlike the accused's lawyer, will be able to see the information and provide adversarial challenge to the *ex parte* submissions made by the Attorney General for non-disclosure under s.38. The use of such security cleared lawyers has not yet been approved by the Federal Court of Appeal. [97] In any event, the appointment of such a person could delay the proceedings. Moreover, a special advocate or other security cleared lawyer will never be as familiar with the accused's case and the possible uses of the undisclosed information as the accused's own lawyers.

Although the Federal Court has been given explicit flexibility under s.38.06 in reconciling competing interests in secrecy and disclosure that include editing and summarizing information as was done in *Khawaja*, creating substitutes for classified information such as the edited transcript used in *Ribic* and making findings against the parties, the ultimate effect of these orders will depend on the judgment made by the criminal trial judge under s.38.14 about the effects of the non-disclosure order on the accused's right to a fair trial. There is a danger that the Federal Court judge may not be in the best position to know the value of information to the accused given that the accused will not have access to the information and the trial often will not have started. In turn, there is a danger that the criminal trial judge may not be in the best position to know the effects of non-disclosure of information on the fairness of the trial. There is no specific mention in either the Attorney General's powers under s.38.03 or the Federal Court judge's powers under s.38.06 of an ability to make an exception to a non-disclosure order that would allow a trial judge to

---

96 *Canada v. Khawaja* 2007 FC 463; *Khadr v. The Attorney General of Canada* 2008 FC 46; *Canada v. Khawaja* 2008 F.C. 560.

97 In upholding the constitutionality of s.38, the Federal Court of Appeal made no mention of the ability of appoint security cleared lawyers to assist in such proceedings. *Khawaja v. Attorney General of Canada* 2007 FCA 388 at para 135. In his concurring judgment, Pelletier J.A. cast doubt on the ability of the court to order that secret information be disclosed to even a security-cleared lawyer when he concluded that under s.38.02 that "the Court could not order and the Attorney General could not be compelled to provide, disclosure of the Secret Information to Mr. Khawaja, or anyone appointed on his behalf in any capacity." Ibid at para 134.

see the undisclosed information.[98] The blind spots of both the Federal Court judge and the trial judge run the risk of causing on the one hand, stays of proceedings that are not necessary to protect the fairness of the trial or, on the other hand, trials that are not fully fair because of the non-disclosure of information that the Federal Court and trial judge did not realize was necessary for the accused to make full answer and defence.

Although an innovative approach was devised between counsel in the Malik and Bagri prosecution in order to avoid Federal Court proceedings, the ultimate dispute resolution process where no agreement is reached involves separate proceedings in Federal Court. Section 38 proceedings will delay and fragment the criminal trial as seen in the *Kevork*, *Ribic* and *Khawaja* case studies discussed in the full paper. They will also not resolve all the disputes as the Attorney General can still claim common law privilege and invoke s.37 of the CEA. In turn, the accused can and will seek a remedy for partial or non-disclosure under s.38.14 of the CEA when the matter returns to the trial judge. As will be seen, other democracies have not duplicated Canada's cumbersome two court process for resolving national security confidentiality claims.

VII. Disclosure and Secrecy in other Jurisdictions

1) The United States

The *Classified Information Procedures Act*[99] was enacted in 1980. It has already influenced s.38 of the CEA in terms of early notification requirements and giving judges a flexible array of options in reconciling the interests in secrecy and disclosure through editing, summaries and substitutions. Nevertheless, it still differs from s.38 in a number of respects. CIPA allows questions of national security confidentiality to be decided by the Federal Court judge who tries terrorism offences. It contemplates that national security confidentiality issues will be factored into general case management questions whereas s.38 of the CEA delegates national security confidentiality issues to a separate court to decide. The trial judge under CIPA is able to revisit initial non-disclosure orders, whereas the trial judge in Canada must accept non or partial disclosure orders made by

---

98 Section 38.05 of the CEA seems to contemplate that a trial judge could make a report to a Federal Court hearing the matter, but does not on its face contemplate a Federal Court judge making a report to a criminal trial judge in order to inform the latter's decision under s.38.14. The Federal Court judge could require the Attorney General of Canada under s.38.07 to notify the trial judge about a non-disclosure order, but this section does not authorize the lifting of the non-disclosure order for the trial judge.

99 PL 96-456

the Federal Court before trial while being able to make necessary orders to protect the fairness of the trial in light of the non-disclosure order.

Another difference between CIPA and the CEA is that CIPA has been interpreted to allow the trial judge in appropriate cases to require defence lawyers to obtain security clearances as a condition of having access to classified information.[100] This procedure has, however, been challenged as restricting the ability of the defence lawyer to reveal the classified information to his or her client and affecting choice of counsel. Nevertheless, the defence lawyer can generally be expected to be in a better position to know the utility of the information to the defence than a special advocate.

Finally, CIPA attempts to manage the inevitable tensions within government between the demands by intelligence agencies for secrecy and the interests of prosecutors in disclosure. It provides several potentially valuable feedback mechanisms so that the government, including legislative committees, is aware of the consequences of overbroad claims of either secrecy or overbroad demands for disclosure. In one post 9/11 terrorism prosecution, the government decided to declassify intercepts 3 days before trials. In response, commentators have recommended that classification of relevant information be reviewed once a prosecution has been commenced in order to respond to chronic overclassification.[101]

2) The United Kingdom

The United Kingdom, like the United States, allows trial judges to make and revisit determinations of national security confidentiality or what they call public interest immunity. The British experience indicates that questions of public interest immunity cannot be divorced from the scope of disclosure obligations. Broad common law disclosure requirements, similar to *Stinchcombe*, have been replaced by narrower statutory disclosure requirements that do not require the disclosure of unused material that is not reasonably capable of undermining the Crown's case or assisting the case for the accused.[102] Unused incriminating intelligence does not have to be disclosed.

---

100 *United States v. Bin Laden* 58 F.Supp.2d 113. To the same effect see *United States v. Al-Arian* 267 F.Supp 2d 1258.

101 Serrin Turner and Stephen Schulhofer *The Secrecy Problem in Terrorism Trials* (New York: Brennan Centre, 2005) at 27, 80.

102 *R v Ward* [1993] 1 WLR 61; *Criminal Procedure and Investigations Act 1996* s.3 as amended by *Criminal Justice Act 2003; R. v. H and C* [2004] UKHL 3 at para 17.

Both the House of Lords in *R. v. H. and C*[103] and the European Court of Human Rights in *Edwards and Lewis*[104] have placed considerable emphasis on the ability of the trial judge to revisit initial decisions that the disclosure of sensitive information is not required in light of an evolving trial including the defence's case and defence cross-examination of witnesses. Although the courts have approached the trial judge's ability to revisit public interest immunity decisions mainly from the perspective of ensuring fairness to the accused, it also has an efficiency dimension because it allows the trial judge to make early non-disclosure orders knowing that, if necessary, they can be revisited. The trial judge can examine the undisclosed material and order non-disclosure, but revisit that order on his or her own motion as the trial evolves in order to ensure a fair trial. This approach is not an option under the two court structure of s.38 of the CEA.

The British have some experience with the use of special advocates in public interest immunity proceedings. At the same time, British courts have warned that the use of special advocates can cause delay and that the special advocate may be unable to take meaningful instructions from the accused after the special advocate has seen the secret and undisclosed information.[105]

3) Australia

Australia has extensive recent experience with claims of national security confidentiality. Its Law Reform Commission prepared an excellent report on the subject[106] and it enacted new legislation to govern national security confidentiality in 2004. The *National Security Information Act*[107] has been controversial and its constitutionality was unsuccessfully challenged.[108] Criticisms have revolved around the Attorney General's power with respect to the initial editing of evidence, the primacy given in the statute to national security over fair trial concerns and the Attorney General's power to require security clearances for defence lawyers. On all these issues, the Australian Law Reform Commission would have given the judiciary more power to make its own determinations of the appropriate means to reconcile secrecy with disclosure.

---

103 [2004] UKHL 3
104 Judgment of October 27, 2004.
105 *R v. H and C* [2004] UKHL 3 at para 22.
106 Australian Law Reform Commission *Keeping Secrets The Protection of Classified and Security Sensitive Information* (2004)
107 *National Security Information (Criminal and Civil Proceedings) Act, 2004*
108 *R. v. Lodhi* [2006] NSWSC 571 at para 85

The Australian Act, like s.38, encourages flexibility in reconciling disclosure with secrecy through the use of devices such as summaries and substitutions. The Law Reform Commission would have provided an even broader menu of alternatives including the ability of witnesses to give anonymous testimony, testimony by way of video or closed circuit television and testimony by written questions and answers. This latter alternative allows vetting for secret information and was used in Canada in the *Ribic* case discussed in the full paper.

The Australian *National Security Information Act* has a number of distinguishing features from the Canadian approach. It gives the trial judge the power to decide issues involving national security confidentiality. It allows for pre-trial conferences to manage the many problems arising from disclosure of national security information. It provides the opportunity for defence lawyers to obtain security clearances. Finally, it allows the trial judge to re-visit issues of disclosure as the trial evolves. The Australian act has already been tested in one completed terrorism prosecution.[109] The judge who presided at that trial has subsequently commented in an extra-judicial speech that:

> There is likely to be an increasing presence of ASIO agents in relation to the collection of evidence to be used in criminal trials involving terrorism. Yet our intelligence agency, for all its skill in intelligence gathering, is perhaps not well equipped to gather evidence for a criminal trial; and its individual agents are not well tutored in the intricacies of the criminal law relating to procedure and evidence. Moreover, the increasing presence of our intelligence agency in the investigating and trial processes brings with it an ever increasing appearance of secrecy which, if not suitably contained, may substantially entrench upon the principles of open justice and significantly dislocate the appearance and the reality of a fair trial.[110]

These comments affirm that establishing a workable relationship between intelligence and evidence is a critical priority for future terrorism trials. They also warn that the need to maintain the secrecy of intelligence will place strains on the criminal trial process.

---

109 See the *R. v. Lodhi* case study in the full paper.

110 Justice Whealy "Terrorism" prepared for a conference for Federal and Supreme Court Judges, Perth 2007.

4) Summary

The above foreign experience provides valuable information for reforming s.38 of the CEA so as to better manage the relationship between secret intelligence and evidence and information that should be disclosed to ensure a fair trial. All three foreign jurisdictions allow the trial judge to decide questions of non-disclosure. This allows issues of non-disclosure to be integrated with pre-trial case management. Even more importantly, it allows a trial judge who has seen the secret material to re-visit an initial non-disclosure order in light of the evolving issues at the criminal trial, a fact that has been emphasized by both the House of Lords and the European Court of Human Rights[111] as essential for the fair treatment of the accused. The ability to revisit non-disclosure decisions also has the potential of allowing the trial to proceed efficiently and not become bogged down in pre-trial disclosure battles.

The comparative experience also reveals some interesting procedural innovations. British courts have allowed the use of special advocates while also indicating some awareness that delay may be caused as the special advocate becomes familiar with the case and that ethical problems may emerge from restrictions on the special advocate's ability to take instructions from the accused after the special advocate has seen the secret information. Both the United States and Australia provide for the alternative of defence counsel being able to examine the sensitive material contingent on obtaining a security clearance and an undertaking that classified material will not be shared with the client. Although the process of obtaining a security clearance could cause delay, it also allows the person most familiar with the accused's case to have access to secret material in order to make arguments about whether its disclosure is necessary for a fair trial. Security clearance requirements adversely affect counsel of choice, but also encourage the use of experienced defence lawyers in terrorism trials. The Australian experience also suggests that the creative use of testimony by closed circuit television can help in reconciling competing interests in disclosure and fairness when members of foreign or domestic intelligence agencies testify in terrorism prosecutions.

---

111 *R v. H and C* [2004] UKHL 3; *Edwards and Lewis v. United Kingdom* Judgment of October 27, 2004.

Conclusions

A) The Evolving Relation Between Intelligence and Evidence

What might be seen as intelligence at one point in time, might be evidence at another point in time.[112] There is a need to re-examine traditional distinctions between intelligence and evidence in light of the particular threat and nature of terrorism and the expanded range of crime associated with terrorism. Terrorism constitutes both a threat to national security and a crime. Although espionage and treason are also crimes, the murder of civilians in acts of terrorism such as the bombing of Air India Flight 182 demands denunciation and punishment that can only be provided by the criminal law. The same is true with respect to intentional acts of planning and preparation to commit terrorist violence. Although attempts and conspiracies to commit terrorist violence have always been serious crimes, the 2001 *Anti-Terrorism Act* has changed the balance between intelligence and law enforcement matters by creating a wide range of terrorist offences that can be committed by acts of preparation and support for terrorism which will occur long before actual acts of terrorism. The prevention of terrorism must remain the first priority, but wherever possible, those who plan, prepare or commit acts of terrorism should be prosecuted and punished. Both Canada's domestic laws and its international obligations demand the prosecution and punishment of terrorism.

There is some concern that CSIS continues to resist the need to gather information in counter-terrorism investigations to evidentiary standards. In contrast, MI5 has the disclosure of information relating to the prevention of serious crime and for criminal proceedings as part of its statutory mandate and it has stated that it will gather some evidence relating to surveillance to evidential standards. With respect to Air India, CSIS information in the form of wiretaps and witness interviews could have been some of the most important evidence in the case, but, unfortunately, they were destroyed in part because of CSIS's understanding of its role as a security intelligence agency that does not collect or retain evidence. The failure to retain and disclose such material can harm both the state's interests and those of the accused.

Although CSIS is not mandated to be a law enforcement agency, s.19(2)(a) of the *CSIS Act* contemplates that it will collect information that will

112 Fred Manget "Intelligence and the Criminal Law System" (2006) 17 Stanford Law and Public Policy Review 415 at 421-422.

have significance for police and prosecutors for investigations and prosecutions and that it may disclose such information to police and prosecutors. There has never been a statutory wall between intelligence and evidence or between CSIS and the police in Canada. Section 18(2) of the *CSIS Act* also contemplates that the identity of confidential sources and covert agents may also be disclosed as required in criminal investigations and prosecutions. Section 12 of the *CSIS Act* should not be taken as authorization for the destruction of information that was collected in accordance with its requirement that information only be collected to the extent that it is strictly necessary. Stark contrasts between the reactive role of the police in collecting evidence and the proactive role of CSIS in collecting intelligence drawn by the Pitfield committee and others have not been helpful. The *CSIS Act* never contemplated an impenetrable wall between intelligence and law enforcement. Although this should have been clear in 1984, it should have been beyond doubt after the Air India bombing, let alone 9/11.

B) The Case Studies: Canada's Difficult Experience with Terrorism Prosecutions

The case studies examined in the full study[113] raise doubts about whether Canadian practices and laws are up to the demands of terrorism prosecutions, particularly as they relate to the relation between intelligence and evidence and the protection of informants. The Parmar prosecution in Hamilton, the Khela prosecution in Montreal and the Atwal prosecution in British Columbia all collapsed because of difficulties stemming from the requirements that the state make full disclosure of relevant information including the identity of confidential informants. The disclosure of the affidavit used to obtain the CSIS wiretap in Atwal disclosed inaccuracies and led to the resignation of the first director of CSIS. The disclosure of the affidavit in the Parmar prosecution also revealed inaccuracies that would have allowed the defence lawyers to cross-examine those who signed the affidavit. Both the Parmar and Atwal cases involved the then novel procedure of giving the accused access to affidavits used to obtain wiretaps and it is hoped that wiretap practice has improved and adjusted to the demands of disclosure. There is an ability to edit affidavits to protect public interests in non-disclosure, but the information that is edited-out cannot be used to support the validity of the warrant. Similarly, witness protection programs have become

113 Kent Roach "The Unique Challenges of Terrorism Prosecutions: Towards a Workable Relation Bteween Intelligence and Evidence" in vol 4 of Research Studies.

more formalized and may have improved since the Parmar and Khela prosecutions collapsed in part because of a reluctance of informers to have their identities disclosed to the accused because of fears for their safety. Nevertheless, these cases underline the likelihood of disclosure when judged necessary for the accused to make full answer and defence and the importance of protecting informers when intelligence is used as evidence in terrorism prosecutions.

The Kevork and Khawaja terrorism prosecutions, as well as the Ribic hostage- taking prosecution, all demonstrate a different type of problem. They were all delayed and disrupted by separate national security confidentiality proceedings in the Federal Court. Section 38 places strains on the prosecution process because it requires the Federal Court to make decisions about non-disclosure without having heard the evidence in the criminal case. In turn, it places strains on a criminal trial judge who is in the difficult, if not impossible, position of deciding whether non or partial disclosure with respect to information that the accused and even the trial judge have not seen will nevertheless adversely affect the accused's right to a fair trial and full answer and defence.

The awkward s.38 procedure was only avoided in the Malik and Bagri prosecution because the experienced counsel on both sides were able to agree on an innovative approach that included inspection of CSIS material by the defence on initial undertakings that it not be shared with their clients. Without this procedure, one that may not be easily duplicated and could require defence lawyers to obtain security clearances, the Malik and Bagri prosecution could easily have been further delayed and perhaps even halted because of the litigation of s.38 issues. A stay of proceedings or another remedy might also have been entered as a response to CSIS's destruction of tapes and witness statements had the trial judge not decided to acquit the accused. In some respects, it was a minor miracle that the case reached verdict.

Attempts have been made to encourage pre-trial resolution of s.38 issues, but the *Ribic* case and the reality of late disclosure in complex cases including the *Khawaja* prosecution suggest that a terrorism prosecution could be beset by multiple s.38 applications and by multiple trips to the Federal Court and appeals to resolve these issues. The United Kingdom and the United States have much more experience with terrorism prosecutions than does Canada and it is noteworthy that they allow the trial judge to make non-disclosure decisions on the grounds of

national security confidentiality. This allows such issues to be integrated into overall trial-management issues and it allows the trial judge to revisit an initial non-disclosure issue should the evolving issues at trial suggest that fairness to the accused requires disclosure. At this point, the prosecution may face the difficult choice of whether to disclose the secret information or to halt the prosecution through a dismissal of charges or a stay of proceedings. This difficult decision, however, will not be made prematurely. It will only have to be made after a fully informed trial judge has decided that disclosure is necessary to ensure fairness towards the accused.

C) Front and Back-End Strategies for Achieving a Workable Relation Between Intelligence and Evidence

Intelligence can be protected from disclosure by not bringing prosecutions or by halting prosecutions, including through a non-disclosure order issued by the Attorney General of Canada under s.38.13 of the CEA. Nevertheless, such non-prosecution strategies are not attractive in the face of deadly terrorist plots that require prosecution and punishment. Leaving aside non-prosecution, there are two broad strategies available to deal with the challenges presented by the need to establish a workable relation between intelligence and evidence.

One broad strategy is front-end and involves changing the nature of secret intelligence to make it usable in criminal prosecutions. These changes would be directed at the practices of CSIS to ensure that where possible they collect intelligence to evidential standards in counter-terrorism investigations and that they consider source and witness protection should it become necessary to disclose the identity of confidential informants. It will also require co-operation between CSIS and the RCMP and other police forces involved in terrorism prosecutions so that Criminal Code procedures, especially with respect to wiretaps, are used when appropriate. The challenges of these front-end reforms, especially to CSIS and to foreign agencies that share information with Canada subject to caveats that the information not be disclosed, should not be underestimated.

The second strategy focuses on the back-end procedures that can be used in court to reconcile the need to keep secrets with the need to disclose material. They involve the rules governing disclosure and production obligations and evidentiary privileges. These reforms are

designed to shield intelligence and other material from disclosure in all cases. Such strategies may attract Charter challenges by limiting disclosure obligations across the board and they risk being held to be over-broad in a particular case. Fortunately, back-end strategies include better-tailored procedures to adjudicate claims of national security confidentiality on the facts of specific cases. It will be suggested that this process can be made more efficient and more fair by focusing on the concrete and specific harms of disclosure of secret information and by allowing trial judges to make, and when necessary to revise, non or modified disclosure decisions.

D) Front-End Strategies to Make Intelligence Useable in Terrorism Prosecutions

1. Collection and Retention of Intelligence With Regard to Evidential and Disclosure Standards

One important front-end strategy is for security intelligence agencies to have more regard for evidentiary and disclosure standards when they collect intelligence in counter-terrorism investigations. The likelihood of prosecution and the possible disclosure or use of some forms of intelligence as evidence has increased since CSIS was created in 1984. This is because the threat of terrorism has increased, disclosure and production standards have increased and many new crimes with respect to the support and financing of terrorism and preparation for terrorism have been created. It will be a rare counter-terrorism investigation where there is not some possibility of a crime being committed and a prosecution being appropriate. This may not necessarily be the case with counter-intelligence or counter-espionage investigations.

In some cases, intelligence agencies such as MI5 and ASIO consciously collect evidence to evidentiary standards in the expectation that their agents may be required to produce such material to the prosecution and to testify in court. The Malik and Bagri prosecutions, however, reveal that CSIS agents at that time did not collect or retain the fruits of their terrorism investigations to evidentiary standards or with a view to a prosecution. Although the acquittal avoided the need to fashion a remedy, the trial judge found that CSIS's failure to retain relevant material including not only the wiretaps but also notes of an interview with a key witness violated Malik and Bagri's rights under s.7 of the Charter. In terrorism investigations, CSIS and other intelligence agencies should constantly

evaluate the likelihood of a subsequent prosecution and the effect that a prosecution could have on secret intelligence. Where possible, they should collect and retain information to evidentiary standards.

Section 12 of the CSIS Act should not have prevented the retention of properly obtained information, but some clarification of s.12 is desirable to make clear that CSIS should retain properly obtained information when it may become relevant to criminal investigations and prosecutions. One option would be to abandon the requirement in s.12 that information and intelligence be collected with respect to activities that on reasonable grounds are suspected of constituting threats to the security of Canada only "to the extent that it is strictly necessary". Such an approach, however, would sacrifice values of restraint and privacy that are protected by the "strictly necessary" standard. A better approach is to make clear that if information is properly collected under the "strictly necessary" standard, it should be retained when it might be relevant to the investigation and prosecution of a criminal offence that also constitutes a threat to the security of Canada. Another option would be to require the retention of information that may be relevant to the investigation or prosecution of a terrorism offence as defined in s.2 of the Criminal Code.

Privacy concerns raised by any increased retention of information can be satisfied by adequate review of the legality of its collection, including the requirement that the collection be "strictly necessary" to investigate activities that may on reasonable grounds be suspected of being threats to the security of Canada. The Inspector General of CSIS, the Security Intelligence Review Committee and the Privacy Commissioner can all review not only the collection of the information but the manner in which it is retained and the manner in which is distributed to other agencies.

Information obtained under a warrant issued under s.21 of the CSIS Act could also be retained at least for the duration of the warrant albeit with restrictions on who has access to the information and with review of any information sharing. There may be a case for judicial authorization and control of information collected under a s.21 wiretap warrant. Retained intelligence should be distributed when required for a criminal investigation or prosecution as contemplated under s.19(2)(a) of the CSIS Act. There may be a case for amending s.19(2) (a) to require CSIS to disclose information that may be used in a criminal investigation or prosecution to the police and to the relevant Attorney General. The idea that CSIS could exercise their present residual discretion to refuse

to disclose such information in order to protect the information from disclosure is problematic. There is a danger that acts of terrorism that could have been prevented by arrests or other law enforcement activity will not be prevented if the information is not passed on to the police. Even a refusal to pass on the information does not guarantee that an accused will not seek disclosure or production if the information becomes truly relevant to a subsequent criminal prosecution. If CSIS does pass on the information, the Attorney General of Canada would still retain the option of seeking a non-disclosure order for the secret information or issuing a non-disclosure certificate under s.38 of the CEA in order to prevent the harms of disclosure.

Although the Air India investigation had unique features that led to CSIS being held to be subject to disclosure and retention of evidence obligations under *Stinchcombe,* it would be a mistake for CSIS to conclude that the fruits of its counter-terrorism investigations could be absolutely protected from disclosure or that CSIS has a discretionary veto on disclosure requirements. Even if CSIS is considered to be a third party for purposes of disclosure, the accused in a terrorism trial may be able to make demands for disclosure of some CSIS material. The courts will impose a slightly higher standard on the accused to obtain production from CSIS as a third party under *O' Connor* than as part of the Crown under *Stinchcombe*, but the courts will still require production when it is required to ensure fairness to the accused.

Some changes in the organizational culture of Canada's security intelligence agencies may be required to deal with the challenges of terrorism prosecutions. The need to protect secrets takes on a new dimension when the targets of intelligence are about to blow airplanes out of the sky. Intelligence agencies must adapt to the new threat environment and the increased possibility that their counter-terrorism investigations may reach a point where it is imperative that the police arrest and prosecute people. Security intelligence agencies must resist the temptation to engage in over-classification and unnecessary claims of secrecy. It is not good enough for security intelligence agencies which are increasingly focusing on counter-terrorism to rely on old mantras that they do not collect evidence.

Security intelligence agencies need to adjust their approaches to disclosure and secrecy to take into account that terrorism is now considered to be the greatest threat to national security and that they will often work

along side the police in trying to prevent terrorist violence. Mechanical and broad approaches to secrecy may have been appropriate during the Cold War when the greatest threat to national security came from Soviet spies, but they are not appropriate in counter-terrorism investigations where the prospect of arrest and prosecution looms large. Starting with the Air India investigation and the *Atwal* case, CSIS has not had a happy experience with disclosure of information to the courts and it must put this unhappy experience behind it. Because of Canada's status as a net importer of intelligence, there may be tendency to err on the side of secrecy over disclosure. Nevertheless, the courts have since *Atwal* placed demands on CSIS for disclosure. More recently, courts are re-examining Cold War concepts such as the fear that a hostile state will piece together various bits of innocuous information through the mosaic effect. They are also recognizing that Canada can ask its allies under the third party rule to consent to the disclosure of intelligence and that the third party rule does not apply to information that is already in the public domain.[114] All of these changes point in the direction of the increased disclosure of intelligence in the future.

Evidentiary standards and disclosure to the court and to the accused, however, will not be possible in all cases. Security intelligence agencies must respect their statutory mandate which is to provide secret intelligence to warn the government about security threats and not to collect evidence. In addition, they must also respect restrictions on the use of intelligence that is provided by foreign agencies and they must protect their confidential informers and their agents. The protection of such information will require back-end strategies to ensure non-disclosure. More effort needs to be made by security intelligence agencies to understand the ability of the legal system to protect secrets from disclosure and to educate other actors and the public about the legitimate needs for secrecy. Justice O'Connor has warned that overclaiming of national security confidentiality could create public suspicion and cynicism about secrecy claims.[115] There needs to be better understanding about the legitimate need to keep secrets with respect to intelligence from our allies, ongoing investigations, secret methods and vulnerable informants.

---

114 *Canada v. Commission of Inquiry* 2007 FC 766; *Canada v. Khawaja* 2007 FC 490.

115 Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar *Report of the Events Relating to Maher Arar Analysis and Recommendations* (Ottawa: Public Works and Government Services) at pp 302, 304

2. Seeking Amendments of Caveats under the Third Party Rule

Canada's status as a net importer of intelligence will continue to present challenges for the management of the relation between intelligence and evidence. Canada must encourage foreign governments to share intelligence with Canada and it must respect caveats or restrictions that foreign states place on intelligence that they share with Canada. That said, the third party rule that honours caveats is not an absolute and static barrier to disclosure when required for terrorism prosecutions. The third party rule simply prohibits the use and disclosure of intelligence without the consent of the agency that originally provided the information.

A front-end strategy that can respond to the harmful effects of caveats on terrorism prosecutions is to work with foreign partners to obtain amendments to caveats that restrict the disclosure of information for purposes of prosecution. Much intelligence that the police receive from foreign and domestic intelligence agencies contains caveats that restrict the subsequent use of that intelligence in prosecutions. The Arar Commission has recently affirmed the importance of such caveats, as well as the need to ensure that intelligence is accurate and reliable. At the same time, it also made clear that amendments to caveats can be sought and obtained in appropriate cases.[116] The recent decision in *R. v. Khawaja*[117] has indicated that the third party rule should not be applied in a mechanical fashion to prevent disclosure of information that was already possessed by Canada or was in the public domain. Even when the third party rule applies, Canada should request permission from foreign agencies to allow the disclosure of information for the limited purposes of terrorism prosecutions. The idea that relationships with foreign agencies or that Canada's commitment to the third party rule will be shaken by even requesting amendments to caveats should be rejected. Foreign agencies who are also facing demands for disclosure in terrorism prosecutions in their own countries, should understand that a request to amend the caveats that they placed on information demonstrates respect for the caveat process. In some cases, foreign agencies may consent to the disclosure or partial disclosure of intelligence. The time lag between the initial collection of intelligence and its possible disclosure in a subsequent

---

116 Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar *Report of the Events Relating to Maher Arar Analysis and Recommendations* (Ottawa: Government Services, 2006) at 318-322, 331-332.

117 2007 FC 490 rev'd on other grounds 2007 FCA 342.

terrorism prosecution may allow caveats to be lifted or amended. In other cases, the foreign agencies will refuse to amend caveats that restrict the subsequent disclosure of information. In such cases, Canada has the tools necessary, including the use of a certificate under s.38.13 of the CEA, to honour its commitments to allies.

3. Greater Use of Criminal Code Wiretap Warrants

Another front-end strategy is to make greater use of Criminal Code authorizations for electronic surveillance in terrorism investigations where prosecutions are expected. The use of such warrants would avoid the questions of whether electronic surveillance conducted by CSIS, the CSE or foreign intelligence agencies would be admissible in Canadian criminal trials. The ATA has made it easier to obtain Criminal Code electronic surveillance warrants in terrorism investigations by eliminating a requirement to establish investigative necessity and extending the duration of the warrants. Such a strategy will, however, require close co-operation between CSIS and the police and a willingness to allow the police to take the lead in a terrorism investigation where grounds exist for obtaining a Criminal Code wiretap warrant.

Criminal Code authorizations present their own challenges relating to the need to disclose much of the information used to obtain the judicial authorization, but the rules relating to disclosure and admissibility are clearer than with respect to security intelligence. The Part VI scheme has been upheld as constitutional by the Supreme Court and the rules and procedures for editing the affidavit to protect public interests in non-disclosure are clear. The same cannot be said about the scheme for CSIS wiretaps which were held to be constitutional in a divided decision by the Federal Court of Appeal twenty years ago.[118] That said, the grounds for editing the affidavit used to obtain a wiretap warrant under s.187(4) of the Criminal Code could perhaps be expanded to allow the deletion of material that would reveal and prejudice intelligence gathering techniques even if disclosure would not endanger the persons engaged in those techniques. Other Criminal Code warrants may also be used in terrorism investigations and judges can order that information relating to such warrants not be disclosed for various reasons listed under s.487.3 of the Criminal Code. These grounds are open-ended and include protection for confidential informants and ongoing investigations, but could be expanded to include the need to protect intelligence gathering

118 *R. v. Atwal* (1987) 36 C.C.C.(3d) 161 (Fed.C.A.).

techniques. State interests in secrecy will have to be reconciled with competing concerns about open courts and fairness to the accused in the particular circumstances of each case. Criminal Code warrant procedures provide an established and constitutional basis for the reconciliation of the competing interests. Material that is edited out of the affidavit used to obtain the warrant and not disclosed to the accused cannot generally be used to sustain the warrant.As will be suggested below, security cleared special advocates could be given access to the unedited affidavit and other relevant material in order to represent the accused's interests in challenging both Criminal Code and CSIS warrants. Such an approach could help protect intelligence and other sensitive material from disclosure to the accused while allowing it to be subject to adversarial challenge.

In appropriate cases the state should continue, as it did in the *Atwal* case, to argue for the admissibility of security intelligence intercepts in criminal trials. These arguments will have a better chance of success in cases where the intelligence was gathered as a part of the intelligence mandate and "the Rubicon" had not been crossed into law enforcement activity. Although Criminal Code authorizations may be possible and helpful in some cases, intelligence agencies still have an important regulatory mandate to collect intelligence through their own special standards. In appropriate cases, intelligence intercepts could be admitted as evidence in criminal trials on the basis that the law authorizing the search is reasonable or that any departure from regular criminal law standards can be justified under s.1 of the Charter given the primary objective of collecting information to inform the government of threats to the security of Canada.

It may also be advisable to amend s.21 of the CSIS Act to make clear that a warrant can be issued to CSIS to conduct electronic surveillance outside Canada. It may be preferable to have CSIS conduct such operations with the consent of the foreign country than to rely on the foreign agencies to conduct such surveillance. The activities of the foreign agency will not be bound by the Charter and they may not have the same priorities or procedures as CSIS. An extra-territorial CSIS warrant can apply to the activities of Canadians who are terrorist suspects whereas CSE will be limited by its mandate to collect foreign intelligence. CSE intelligence gathered under a Ministerial authorization is less likely to be admitted as evidence than CSIS intelligence gathered under a judicial warrant.

Even if the use of an intelligence intercept or a Criminal Code wiretap was found by the courts to result in an unjustified violation of rights against

unreasonable search and seizure, the evidence obtained could in some cases still be admitted into a criminal trial under s.24(2) of the Charter. The *Parmar* prosecution might have continued had the state been able to rely on section 24(2). The state could have argued that it relied in good faith on the warrant even if the warrant could not be sustained and was invalid after the information in the affidavit that identified the informant was edited out. Section 24(2) will not, however, work in all cases and might not have worked in *Parmar* if the court had concluded that there was a serious violation of the Charter.

4. Greater Use of Source and Witness Protection Programs

A final front-end strategy to make intelligence more usable in criminal prosecutions is the use of enhanced witness protection programs by both security intelligence agencies and police forces. Such programs are designed to make it possible for confidential informants when necessary to have their identity disclosed and to testify in criminal prosecutions. They should also when necessary provide protection to informants who may not testify but whose identity might be revealed by disclosure requirements. The *Parmar* prosecution collapsed because of the unwillingness of a key informant to have his identity disclosed. Many of the disclosure problems in the *Khela* prosecution stemmed from the apparent agreement of the police that the key informant would not have to testify. Informants have many good reasons not to testify and there is no magic solution. Nevertheless, all reasonable efforts should be made to make it possible and attractive for them to testify.

Security intelligence agencies should be able to draw on the resources of witness protection programs. International relocation may be especially important in international terrorism prosecutions. Increased efforts should be made to ensure that the difficulties faced by witnesses are better understood by all. The importance of adequate and effective source and witness protection in managing the relation between evidence and intelligence cannot be easily overstated.[119]

---

119 The most recent annual report on the federal witness protection run by the RCMP indicates that $1.9 million was spent on it and while fifty-three people were in the program, fifteen witnesses refused to enter it, twenty-one voluntarily left the program and seven were involuntarily removed from the program. Witness Protection Program Annual Report 2005-2006 at http://securitepublique.gc.ca/abt/dpr/le/wppa2005-6-en.asp See also Yvon Dandurand "Protecting Witnesses and Collaborators of Justice in Terrorism Cases" in vol 3 of the Research Studies.

E) Back-End Strategies To Reconcile The Demands of Disclosure and Secrecy

Although front-end strategies to make intelligence more usable in criminal prosecutions need to be developed, there is also a need for back-end strategies that can prevent the disclosure of information that if disclosed will result in serious harm. The disclosure of secret intelligence that is not necessary to ensure a fair trial should not occur given the compelling need to protect informants, security intelligence investigations and operations and the vital free flow of secret information from our allies. Whereas the burden of devising and implementing front-end strategies to make intelligence more useable in terrorism prosecutions fall largely on intelligence agencies and the police, the burden of back-end strategies generally fall on prosecutors, defence counsel, courts and legislatures.

1. Clarifying Disclosure and Production Obligations

One back-end strategy is to clarify the extent of disclosure requirements on the Crown and to provide legislative guidance for requests for production from CSIS when it is determined to be a third party not subject to *Stinchcombe*. A number of the terrorism prosecutions examined in this study were undertaken before the Supreme Court's landmark decision in *Stinchcombe* which requires disclosure of relevant and non-privileged evidence or the Court's recognition in *O'Connor* of a procedure for producing and disclosing material from third parties when required for a criminal trial. Although disclosure standards existed under the common law before *Stinchcombe*, there is a need for as much clarity as possible about the extent of disclosure requirements. Some clarity has been achieved as a result of the amendments governing the opening of the sealed packet under Part VI of the Criminal Code, but more work remains to be done. In its late 1990's study of RCMP/CSIS co-operation, SIRC reported perceptions that any information that CSIS passed to the RCMP would be subject to *Stinchcombe* disclosure requirements. Although *Stinchcombe* imposes broad disclosure obligations, those obligations are not unlimited. The Crown need only disclose information that is relevant to the matters raised in the prosecution. The standard of relevance is higher with respect to *O'Connor* demands for production from third parties. In addition, some balancing of interests is allowed before disclosure of third party records. Information protected by privilege such as the informer privilege, is generally not subject to disclosure. Disclosure can be delayed for legitimate reasons relating to the safety of witnesses and sources and

ongoing investigations. Finally, the courts have distinguished between violations of rights to disclosure and more serious violations of the right to full answer and defence.

There is a need for better understanding and codification of disclosure principles. Given the breadth of terrorism offences and the value of having universal rules that apply to all crimes, it may be advisable to codify disclosure principles for all prosecutions. *Stinchcombe* was decided more than fifteen years ago and even at that time, the Court seemed to expect some subsequent codification of the details of disclosure. Greater certainty about the ambit of disclosure requirements and the legitimate reasons for not disclosing information would assist in terrorism prosecutions. The comparative experience of the United Kingdom suggests that there may be considerable advantage in codifying disclosure obligations. The courts in that country proclaimed broad common law standards of disclosure in part out of a recognition that a failure to make full disclosure had resulted in miscarriages of justice in a number of terrorism cases. Parliament, however, subsequently clarified disclosure obligations and the Crown now need not disclose material in any case, including secret intelligence in terrorism cases, unless it can reasonably be capable of undermining the case for the prosecution against the accused or of assisting the case for the accused.[120] In short, it is not necessary in the United Kingdom to disclose unused but incriminating intelligence.

It will be more difficult to codify and restrict disclosure standards in Canada than in the United Kingdom because the courts have held that the accused has a constitutional right under s.7 of the Charter to disclosure of relevant and non-privileged information. The courts will accept the need to protect legitimate secrets as an objective that is important enough to justify restricting Charter rights, but the critical issue will be whether restrictions on disclosure are the most proportionate means of advancing this important objective. Courts may well look to the process under ss.37 and 38 of the CEA as a less drastic and more tailored means to secure non-disclosure of secrets by judicial order after a judge has examined the secret material in light of the facts of the particular case.

It is also possible for Parliament to legislate in relation to the procedure and standards to be applied when the accused seeks production and disclosure of records held by third parties. Although CSIS was held to

120 *R v Ward* [1993] 1 WLR 61; *Criminal Procedure and Investigations Act 1996* s.3 as amended by *Criminal Justice Act 2003; R. v. H and C* [2004] UKHL 3 at para 17.

be subject to *Stinchcombe* in the unique circumstances of the Air India investigation, it may be held to be a third party in other cases. Legislation to deem CSIS to be a third party not subject to *Stinchcombe* is also a possibility, but one that could be challenged under s.7 of the Charter on the facts of individual investigations. In cases where CSIS is a third party not subject to *Stinchcombe*, the Court in *Mills* made clear that Parliament can alter the common law procedure in *O'Connor* which requires the accused to show that material is likely relevant and that the interests in disclosure are greater than the interests in non-disclosure. For example, it might be possible to clarify that matters relating only to the internal workings of intelligence agencies are not relevant enough to require disclosure to the defence. It may also be possible to instruct courts to consider certain factors, such as the harmful effect of disclosure on informants, commitments made to foreign states and ongoing investigations before ordering production and disclosure. Nevertheless, any new scheme to govern the production of intelligence would have to comply with the accused's right to full answer and defence.

The courts have already accepted that not every violation of the accused's right to disclosure will violate the even more fundamental right of full answer and defence. The courts may be prepared to accept some legislative limits on disclosure rights, especially when disclosure would harm state interests in national security. That said, the courts are also attentive to the cumulative adverse effects on the accused's right to full answer and defence when the accused is denied access to relevant information and information that could open up avenues for the defence. It is important that independent judges be the ultimate decision-maker about the disclosure of information because state officials have an incentive to maximize secrecy. As a result of noble-cause corruption or tunnel vision, state officials may fail to disclose information that may be valuable to the accused. A failure to make full disclosure has been an important factor in wrongful convictions, including in terrorism cases.

Legislative restrictions on disclosure or production will be challenged under the Charter. Even if upheld under the Charter, the accused will frequently argue that the state has failed to satisfy disclosure or production obligations codified in new legislation. Such arguments could delay terrorism prosecutions. Courts will not and should not return to earlier practices of ordering non-disclosure of intelligence material without even examining the material to determine its value to the accused.

2. Clarifying and Expanding Evidentiary Privileges that Shield Information from Disclosure

A related strategy to reduce disclosure and production obligations is the codification and expansion of privileges like the police informer privilege or the creation of new privileges. There may be a case for some codification and perhaps expansion to make clear that CSIS informers also enjoy the benefit of police informer privilege, but there are limits to this strategy. Even the most zealously guarded privileges such as the police informer privilege are subject to innocence at stake exceptions.[121] There is an understandable reluctance to create new class privileges and case-by-case privileges may provide little advance certainty about what is not to be disclosed. There is also a danger that new privileges will encourage the non-disclosure of information that is necessary for full answer and defence. If privileges are dramatically expanded, courts will likely make increased use of innocence at stake or full answer and defence exceptions to the expanded privilege. The end result may be that an expanded privilege may be less certain and perhaps even less protective of the state's interest in non-disclosure.

Placing too much reliance on legislating narrower disclosure or production rights or expanding privileges may invite both Charter challenges and litigation over whether information fits into the new categories. Rather than attempting the difficult task of imposing abstract limits in advance of the particular case on what must be disclosed to the accused and risking that such limits may be declared unconstitutional or spawn more litigation, a more practical approach may be to improve the efficiency of the process that is used to determine what must be disclosed and what can be kept secret within the context of a particular criminal trial. That said, presumptive privileges could have the benefit of providing some certainty to the agencies, in particular CSIS, that information could be shared with the police without necessarily being disclosed. Any new privilege would have to be defined with as much precision as possible and it would be subject to litigation to determine its precise ambit. It should also be subject to an innocence at stake exception.

---

121 *R. v. Leipert* [1997] 1 S.C.R. 287; *Named Person v. Vancouver Sun* 2007 SCC 43.

3. Use of Special Advocates to Represent the Interests of the Accused in Challenging Warrants while Maintaining the Confidentiality of Information Used to Obtain the Warrant

Electronic surveillance can provide some of the most important evidence in terrorism prosecutions, especially in cases where it may be difficult and dangerous to use human sources. Both the *CSIS Act* and the *Criminal Code* provide means to obtain wiretap warrants. Both provisions have been sustained under the Charter, but courts have stressed that the general rule is that there should be full disclosure of the affidavits used to obtain the wiretap warrant. The affidavit can be edited to protect a broad range of public interests in non-disclosure including the protection of informants and ongoing investigations. This protection of information from disclosure, however, comes with a price. Any material that is edited out of the affidavit and not disclosed to the accused or perhaps summarized for the accused cannot be used to support the legality and constitutionality of the wiretap. Material that has been edited out and not known to the accused cannot be effectively challenged by the accused. In some cases, the editing may mean that the warrant is not sustainable and that the wiretap evidence can only be admitted if a judge determines that its admission would not bring the administration of justice into disrepute under s.24(2) of the Charter.

The use of security-cleared special advocates in proceedings to challenge wiretap warrants may make it possible to provide adequate protection for the accused's right to challenge the warrant as part of the accused's right to full answer and defence and right against unreasonable searches while not disclosing to the accused information that would compromise ongoing investigations, confidential informants or secret intelligence. Special advocates at present play a role under immigration law security certificates, but the role that they could play with respect to challenging warrants could be less problematic. Special advocates would be standing in for the accused only for the limited purpose of challenging the search and arguing that the evidence should be excluded. [122] A special advocate should be in a good position to make an effective adversarial challenge to the warrant. Indeed, the special advocate could be in a better position than the accused to challenge the warrant to the extent that the special

---

122 The Supreme Court has stressed the differences between proceedings where the basis for granting a warrant are challenged and a trial on the merits where the accused has full rights of cross-examination and the Crown must prove guilt beyond a reasonable doubt. *R. v. Pires; R. v. Lising* [2005] 3 S.C.R. 343 at paras 29-30.

advocate sees information that would normally be edited out. Finally, any evidence that the Crown would lead in a terrorism prosecution, including the results of a wiretap should it be found to be admissible, would still have to be disclosed to the accused to ensure a fair trial. Special advocates could act in the accused's interests in challenging the warrant, but they would not act for the accused during the actual trial.

A security-cleared special advocate could be given full access to the unedited affidavit used to obtain a warrant whereas now the accused only sees an edited version of the affidavit. The special advocate could also have access to other material that is relevant to challenging the wiretap warrant, including *Stinchcombe* material disclosed to the accused. The special advocate could in appropriate cases conduct cross-examinations on the affidavit. The special advocate's access to the full affidavit would respond to the concerns of the Supreme Court that the editing of the affidavit while necessary to protect important law enforcement interests, should be kept to a minimum.[123] The special advocate could be briefed by the accused's lawyer about the case before the challenge to the warrant started. The special advocate could also under existing practice seek the permission of the presiding judge to ask relevant questions of the accused or his counsel in order to challenge the warrant if this was necessary after the special advocate had seen the unedited affidavit. Such a process would have to be done with care particularly if the special advocate's questions could reveal the identity of an informant or an ongoing investigation. The use of a special advocate could allow the trial judge (who would also have to be authorized to see and hear the secret material) to hear full and informed adversarial challenges to the warrant without disclosing confidential information used to obtain the warrant to the accused or to the public. Information from the warrant that was admitted into evidence in the criminal trial would continue to be disclosed and challenged by the accused and not the special advocate.

4. Confidential Disclosure and Inspection of Relevant Intelligence

At present, lawyers for the accused are placed in the difficult position of making very broad claims for disclosure of intelligence that they have not seen. As will be seen in the next section, the accused's overbroad claims for disclosure are sometimes met with similarly overbroad claims of secrecy. The relation between intelligence and evidence may become more solid if both sides can be encouraged to make more informed and disciplined claims.

---

123 *R. v. Durette* [1994] 1 S.C.R. 469

In the *Malik and Bagri* prosecution, defence counsel were allowed to inspect CSIS material on an undertaking that they would not disclose the information to their clients unless there was agreement with the prosecutors or a court order for disclosure. Agreement about disclosure was reached in that case and it was not necessary to litigate these issues in the Federal Court under s.38 of the CEA. In future cases, it may be advisable to allow defence counsel to be able to inspect secret material subject to an undertaking that they will not share that information with their client until disclosure has been approved by the Attorney General of Canada or the court. In such cases, there will be a need to ensure the confidentiality of the material that is disclosed and this may require the defence counsel to be provided with access to secure locations and secure equipment.

There may also be a case for requiring defence counsel to obtain a security clearance before obtaining access to secret material. Such a process could delay prosecutions and adversely impact choice of counsel. These problems should not be insurmountable if there is an experienced cadre of defence lawyers with security clearances and with adequate facilities and funding to conduct a defence. Security clearances for defence lawyers are used in both Australia and the United States. Some of Canada's new special advocates also act as defence counsel.

In cases where a defence lawyer is not willing or able to obtain a security clearance, a security-cleared special advocate could be appointed to see the secret information and challenge the Attorney General's *ex parte* submissions for non-disclosure.[124] The appointment of a special advocate would also add further delay to s.38 proceedings, albeit delay related to becoming familiar with the case and not with respect to obtaining a security clearance. The special advocate may never be as familiar with the possible uses of the undisclosed secret information to the accused as the accused's own lawyer. A special advocate could, however, effectively challenge overbroad claims of national security confidentiality and in that way produce material that could be disclosed to the accused. A special advocate would not be used, as is the case under immigration law, to

124 *Canada . v. Khawaja* 2007 FC 463. See also *Khadr v. Canada* 2008 FC 46 and *Canada v. Khawaja* 2008 FC560 appointing a security cleared lawyer in s.38 proceedings.

challenge evidence that is not seen by the accused.[125] As the Supreme Court recognized in *Charkaoui*, s.38 of the CEA does not authorize the use of secret evidence not seen by the accused. Any extension of the use of secret evidence to criminal proceedings would violate the accused's right to a fair trial under ss.7 and 11(d) of the Charter. It would be difficult if not impossible to justify under s.1 given the more proportionate and more fair alternatives of obtaining selective non-disclosure orders on the basis of harms to national security or of prosecuting the accused for another terrorism or criminal offence that would not require the use of secret evidence.

Although special advocates may play a valuable role in s.38 proceedings before the Federal Court in challenging the government's case for secrecy and non-disclosure, it is not clear what, if any, role they would play when a criminal trial judge has to decide under s.38.14 whether a remedy is required to protect the accused's fair trial rights in light of the Federal Court's non-disclosure order. The security-cleared special advocate will have seen the secret information that was the subject of the non-disclosure order, but under the present law will not be able to inform the criminal trial judge about this information. The accused will not be subject to such restrictions, but will not have seen the information that was the subject of the non-disclosure order. The process would be simplified if the trial judge was allowed to see the secret information that was the subject of the non-disclosure order.

5. A Disciplined Harm-Based Approach to Secrecy Claims

There is a danger that overbroad demands for disclosure by the accused in terrorism prosecutions may be matched by overbroad demands for secrecy by the Attorney General of Canada. There have been a number of recent disputes over whether the Attorney General of Canada has engaged in overclaiming of national security confidentiality. The disputes between the Arar Commission and the Attorney General of Canada were resolved during the inquiry and by a decision of the Federal Court that authorized

---

125 The joint committee of the British House of Lords and House of Commons On Human Rights has been critical of the use of special advocates in other contexts, but has concluded that they are appropriate in the similar context of applications for public interest immunity. It has stated: "Public interest immunity decisions are not about whether the prosecution has to disclose the case on which it relies to the defence; rather, such decisions concern whether the prosecution is obliged to disclose material on which it does not rely, which might assist the defence. When deciding a public interest immunity claim, recourse can be had to court appointed special advocates." Joint Committee on Human Rights *Counter-Terrorism Policy and Human Rights: Prosecution and Pre-Charge Detention* July 24, 2006 at para 105.

the release of the greater part of the disputed information.[126] Over use of national security confidentiality claims can produce public cynicism and suspicion about even legitimate claims of secrecy. When there are legitimate secrets that must be kept to protect vulnerable informants, ongoing investigations and promises to allies, there is a danger that the wolf of national security confidentiality may have been cried too often.

One means of addressing concerns about the legitimacy of national security confidentiality claims would be to narrow the ambit of s.38 which requires justice system participants to invoke its processes over a wide range of material that the government is taking measures to safeguard even if there is not a potential for actual injury to a public interest. Another means would be to specify the precise harms of disclosure to the public interest. Section 38.06 at present requires that the disclosure of the material would be injurious to national security, or national defence or international relations. The courts have attempted to define these terms,[127] but they remain extremely broad and vague. More precise definition of the harms of disclosure, or even specific examples of harms to national security or international relations, might help prevent overclaiming. It could also educate actors about the legitimate needs for secrecy with respect to matters such as the protection of vulnerable sources, ongoing investigations and promises made to allies that intelligence would not be disclosed or used in legal proceedings. A harm-based approach could respond to the concerns articulated by the Arar commission and some judges that the government has invoked s.38 in situations where the injury that would be caused by disclosure has not been established.

Section 38 could also be amended to recognize the evolving distinction between intelligence and evidence. The third party rule should not apply if the information was already in the public domain or known to Canadian officials. Even when the third party rule applies, the government could be required to make reasonable efforts to obtain consent from the originating agency to the disclosure of the caveated material. Courts

---

126 *Canada v. Commission of Inquiry into the Activities of Canadian Officials in Relation to Maher Arar* 2007 FC 766. See also *Canada v. Khawaja* 2007 FC 490 and *Canada v. Khawja* 2008 FC 560 for expression of concern that the government has made secrecy claims where injury to national security from disclosure has not been established.

127 National security has been defined the "means at minimum the preservation in Canada of the Canadian way of life, including the safeguarding of the security of persons, institutions and freedoms" *Canada v. Commission of Inquiry* 2007 FC 766 at para 68. National defence includes "all measures taken by a nation to protect itself against its enemies" and "a nation's military establishment". International relations "refers to information that if disclosed would be injurious to Canada's relations with foreign nations." Ibid at paras 61-62.

have also recognized that claims that evidence should not be disclosed because of the "mosaic effect" should be approached with caution. [128] Concerns about the mosaic effect have their origins in the Cold War and may not be as applicable in prosecutions of loosely organized non-state actors such as terrorists. Finally, the harms of non-disclosure could be specified especially in relation to the right to full answer and defence. Attention should be paid to the cumulative effects of non-disclosure on the ability of the accused to undermine the Crown' case and advance defences, as well as on the fairness of the process.

A more restrained and harm-based approach to secrecy claims under s.38 of the CEA, perhaps accompanied by a willingness to allow defence counsel to inspect some secret material on condition of not disclosing the material to their clients without further agreement and perhaps after obtaining a security clearance, could decrease the need to litigate secrecy and disclosure issues under s.38 of the CEA. That said, the Attorney General of Canada will have to insist that some secret material not be disclosed and the competing interests in disclosure and non-disclosure will have to be determined under s.38. It is important that the process for reconciling the interests in disclosure and non-disclosure be both fair and efficient.

6. An Efficient and Fair One Court Process for Determining National Security Confidentiality Claims

In my view the most important back-end strategy in managing the relationship between intelligence and evidence is to make the process for seeking non or modified disclosure orders in individual case more efficient and more fair for all parties. Such a reform will respond to the limits of front-end strategies in making it easier to use intelligence as evidence as well as responding to the limits of attempts to reduce disclosure requirements through legislation or the creation of new privileges. The s.38 process should evolve to allow trial judges to decide on the facts of the particular case whether and when disclosure of secret material is necessary for a fair trial. Such an approach follows the best practices of other democracies with more experience with terrorism prosecutions than Canada.

Although public interest immunities can be asserted before superior court trial judges under s.37 of the CEA, national security, national defence and

128 ibid; *Canada v. Khawaja* 2007 FC 490

international relations claims can only be asserted before the Federal Court under s.38 of the CEA. Criminal trial judges must respect the orders made by the Federal Court with respect to disclosure, but they also retain the right to order whatever remedy is required, including a stay of proceedings, to protect the accused's right to a fair trial. The *Kevork*, *Ribic* and *Khawaja* case studies underline the difficulties of Canada's two court structure. Although the trial judge in *Kevork* ultimately held that a fair trial was possible after the Federal Court refused to order the disclosure of CSIS material, he expressed much uneasiness about the bifurcated process. It is inherently difficult to ask a trial judge to conclude that disclosure of information that he or she has not seen is not necessary to ensure the fairness of the trial. At a minimum some way must be found to ensure that the trial judge and perhaps a security cleared lawyer can examine relevant secret information that has not been disclosed to the accused.

The *Ribic* prosecution demonstrates that s.38 issues can arise in the middle of a trial. In that case, a mistrial was declared when the issues were litigated in Federal Court and an appeal heard by the Federal Court of Appeal. A new trial was held, but the entire process took six years to complete. Section 38 was amended in 2001 to require pre-trial notification of an intent to disclose or call classified information. Despite best efforts by all concerned, however, s.38 issues can emerge later in a criminal trial. For example, the Crown has a reviewable discretion to delay disclosure if required to protect witnesses. The accused may also wish to call evidence that might implicate s.38 of the CEA. A trial judge may have difficulty denying the accused the ability to call evidence that is necessary for full answer and defence. Although the Crown could be penalized for late disclosure, a refusal to allow the Crown to make a s.38 claim with respect to late-breaking disclosure could force it to abandon the prosecution in order to keep the information secret. The litigation of national security confidentiality claims in the Federal Court either before or during a criminal trial can threaten the viability of a terrorism prosecution. The accused has a right to a trial in a reasonable time and the public, including the jury, has an interest in having terrorism trials resolved in a timely manner. The delays in the *Khawaja* prosecution are a matter of concern especially when compared to completion of the trial of his alleged co-conspirators in Britain.

Even if delay problems can somehow be avoided through an expedited s.38 process, the two court approach places both the Federal Court and trial judges in difficult positions. The Federal court judge must attempt to determine the importance of non- disclosed information to the accused

when the accused's lawyer has not seen the information and at a pre-trial stage when the issues that will emerge at trial may not be clear. The ability of the defence to make *ex parte* submissions to the Federal Court judge cannot compensate for the fact that the defence has not seen the undisclosed evidence and the trial evidence has not yet taken shape. Even the possibility that a security cleared special advocate may be appointed to challenge the government's case for non-disclosure cannot guarantee the disclosure of all information that should be disclosed. Even if the Federal Court judge had the advantage of full adversarial arguments on non-disclosure motions, the judge would still have the burden of making final decisions about non-disclosure and partial disclosure without knowing how the criminal trial might evolve. Judges who make similar non-disclosure decisions in Australia, the United Kingdom and the United States all take great comfort in the fact that they can revisit their non-disclosure decisions in light of emerging evidence and issues at trial.

The criminal trial judge is in an equally difficult position under the unique two court structure of s.38 of the CEA. The trial judge must decide that a fair trial is possible without the disclosure of information that the accused, the accused's lawyers and likely the trial judge have not seen. Conversely, the trial judge must fashion a remedy, including perhaps a stay of proceedings, for non-disclosure of the secret information. Although the trial judge might be guided by a schedule that lists the information that was subject to the non-disclosure order, that schedule itself cannot contain identifying information that would cause injury to national security or national defence or international relations.[129] Although the trial judge can issue a report to the Federal Court judge under s.38.05 and the Federal Court can apparently remain seized of the s.38 matter during the trial, [130] the two court structure remains cumbersome and unprecedented outside Canada.

One possible argument in favour of the present two court system is that it provides a form of checks and balance between the two courts and ensures that the trial judge is not tainted by seeing the secret information that the Federal Court has ordered not be disclosed. No concerns have, however, been raised in other countries that judges will be influenced in their decisions by the information that they have seen, but ordered not to be disclosed. In many cases, the material will simply be intelligence that the Crown has found not to be necessary to be used as evidence.

---

129 *Canada. v. Khawaja* 2007 FCA 342 at para 12.
130 *Canada v. Khawaja* 2008 FC 560.

Judges are routinely trusted to disregard prejudicial but inadmissible information about the accused including coerced or unconstitutionally obtained confessions. In any event, the accused will also have the right to a trial by jury.

Canada's unique two court approach runs the risk of decisions in both the Federal Court and the trial court that either prematurely decide that disclosure is not necessary or alternatively that prematurely penalize the prosecution for failing to make disclosure that is not actually required in order to treat the accused fairly. In short, the bificurated court structure is a recipe for delay and disaster in terrorism prosecutions.

No other democracy of which I am aware uses a two court structure to resolve claims of national security confidentiality. Australia, the United Kingdom and the United States all allow the trial judge to decide whether sensitive information can be withheld from disclosure without compromising the accused's rights. This approach is attractive because it allows trial judges to make non-disclosure orders knowing that they can revise such orders if fairness to the accused demands it as the trial progresses.

A One Court Approach: Superior Trial Court or Federal Court?

Reforms of the two court Canadian approach could proceed in two directions. It is perhaps possible to give the Federal Court jurisdiction over all terrorism prosecutions. This approach, however, would require that the Federal Court be given jurisdiction to sit with a jury or it would attract challenge under s.11(f) of the Charter. The expansion of Federal Court jurisdiction or an attempt to create a new court to hear terrorism cases could also attract challenge under s.96 of the Constitution Act, 1867 as infringing the inherent core criminal jurisdiction of the provincial superior courts. The expansion of Federal Court jurisdiction to include criminal terrorism trials or the creation of a new terrorism court could be supported by an argument that terrorism, like youth justice, is a novel matter that did not exist in 1867. As such, it could be transferred away from the superior trial courts.[131] Nevertheless, there are stronger arguments that terrorism has been around for a long time and that terrorism prosecutions in essence involve attempts to punish murder including conspiracy and attempted murder. From 1867 to the present, only superior trial courts

131 *Reference re Young Offenders* [1991] 1 S.C.R. 252.

in the provinces have tried murder charges before juries.[132] Murder, like contempt of court and perhaps treason, sedition, and piracy, are matters within the core jurisdiction of the superior trial courts in the provinces. As such, they cannot be changed by Parliament or the provinces without a constitutional amendment. Removing jurisdiction from the provincial superior courts to try the most serious crimes, terrorist acts of murder or preparation or facilitation of such acts, could be held to violate s.96 of the Constitution Act, 1867.[133] The Federal Court or a new terrorism court would still be conducting terrorist trials for traditional purposes of determining guilt and punishment as opposed to distinct purposes such as developing a system of youth justice. Even if s. 96 did not prevent a transfer of core superior court jurisdiction to another federal court, the power to constitute courts of criminal jurisdiction to try terrorism crimes is arguably a matter of provincial jurisdiction.[134]

Even if constitutionally permissible, such an approach would also require the Federal Court to develop and maintain expertise in criminal law, criminal procedure and criminal evidence matters. This could be difficult if terrorism prosecutions remain infrequent. A former general counsel to the Central Intelligence Agency, Fred Manget, has rejected calls for the Foreign Intelligence Surveillance Court (which issues foreign intelligence wiretaps) to conduct criminal terrorism prosecutions. He has argued that although the special court "operates with admirable secrecy, it was not meant to conduct trials. Instead, it was designed to establish the existence of probable cause, based only upon the government's ex parte appearance. Mixing the probable cause determination with an adversarial trial could raise due process or impugn the impartiality of subsequent trials."[135] In other words, it is better to build national security expertise

---

132 See *Criminal Code* s.469.

133 *MacMillan Bloedel Ltd. v. Simpson* [1995] 4 S.C.R. 725 at para 15 ("The superior courts have a core or inherent jurisdiction which is integral to their operations. The jurisdiction which forms this core cannot be removed from the superior courts by either level of government, without amending the Constitution). (emphasis added) The dissent rejected the idea of core jurisdiction in that case, but also found that jurisdiction being removed from the provincial superior court to punish young people for contempt of court was ancillary to special powers exercised by youth courts.

134 Peter Hogg has suggested that s.96 should not prevent the transfer of core superior court jurisdiction to another federal court. Peter Hogg *Constitutional Law of Canada* 4th ed at 7.2(e) But *MacMillan Bloedel Ltd. v. Simpson* [1995] 4 S.C.R. 725 at para 15 indicates that the core jurisdiction of the superior courts "cannot be removed from the superior courts by either level of government, without amending the Constitution." In any event, Professor Hogg also indicates that the federal government does not have jurisdiction to constitute or establish courts of criminal jurisdiction, a matter expressly excluded from the federal power over criminal law and procedure under s.91(27) and included in the provincial power over the administration of justice under s.92(14). See ibid at 19.3. The only federal power that would support the creation of a new court to try terrorism cases would seem to be the somewhat uncertain residual power to make laws for peace, order and good government.

135 Fred Manget "Intelligence and the Criminal Law System" (2006) 17 Stanford Law and Public Policy Review 415 at 428.

into the existing criminal trial courts than to attempt to give a court with national security expertise but no criminal trial experience the difficult task of hearing terrorism trials.

Having terrorism prosecutions heard in the Federal Court or the creation of a new court would also raise concerns about special terrorism courts, concerns that have surrounded the Diplock courts in Northern Ireland and special courts in Ireland. One of the values of terrorism prosecutions is that they allow terrorist acts of violence to be denounced as crimes and terrorists to be punished and stigmatized as criminals. At this level, at least, terrorists should not be elevated to the status of a political challenge to the state that requires special solutions such as special courts.

A preferable approach would be to give designated judges of the superior trial court who have extensive experience with complex criminal trials the ability to determine national security confidentiality claims under s.38 of the CEA during a terrorism trial. This could be done by amending the definition of a judge under s.38 to include a judge of the provincial superior court when a national security confidentiality matter arises before or during a criminal trial. Because of the need for secure facilities and training with respect to national security confidentiality, not all provincial superior court judges would have to be designated as judges under s.38 of the CEA. The Chief Justice of each provincial superior court could designate a few judges who would be able to make decisions under s.38 of the CEA for the purposes of criminal trials. This could also have the effect of allowing such a trial judge to be assigned to a terrorist case at the earliest possibility in order to help case manage complex terrorism prosecutions.

Superior court trial judges can already decide public interest immunity claims under s.37 and they should be able to learn enough about national security matters to make s.38 decisions. The Attorney General of Canada would still have the opportunity to make ex parte arguments to these judges about the dangers of disclosing information. These judges could also be assisted by adversarial argument on s.38 issues provided by the accused and by security-cleared special advocates who had examined the secret material. Finally, the Attorney General of Canada would still have the power under s.38.13 of the CEA to block a court order of disclosure of material that relates to national security or national defence or was received from a foreign entity.

It could be argued that the Federal Court should retain responsibility in all s.38 matters because of its expertise and the need to reassure allies that secret information will be treated with appropriate care. If this argument was accepted, it would still be possible to appoint select provincial superior courts judges as deputy judges of the Federal Court with the consent of their Chief Justice, the Chief Justice of the Federal Court and the Governor in Council.[136] Such judges would have to acquire expertise with respect to matters affecting national security confidentiality.[137] In addition, it might be easier for provincial superior court trial judges who were designated as deputy judges of the Federal Court to use the secure facilities of the Federal Court.

Allowing provincial superior court trial judges designated by their Chief Justice to decide national security confidentiality or public interest immunity questions would be consistent with the approaches taken in Australia, the United Kingdom and the United States. Such an approach could develop specialized expertise among a small number of trial judges with respect to all aspects of the management of terrorism trials including s.38 issues.[138] Measures would have to be taken to ensure that superior court trial judges designated to decide s.38 issues that arise in a criminal trial would have the appropriate facilities and training for the storage of classified information and that they would have the opportunity to develop expertise on complex matters of national security confidentiality. If necessary, terrorism trials could under s.83.25 of the Criminal Code be prosecuted by the Attorney General of Canada in Ottawa, even if the offence is alleged to have been committed outside of Ontario.

This single court approach would allow trial judges to manage all disclosure aspects of complex terrorism prosecutions without artificial separations between s.38 matters that have to be decided in the Federal Court and other disclosure matters including those under s.37 that have to be decided by the trial judge. It would also stop the duplication of proceedings that may be caused by having preliminary disputes and appeals decided under s.38 only to have the same or similar issues potentially resurface before the trial judge under s.37 or s.38.14 of the CEA. A one court approach could help establish a solid institutional foundation

---

136 *Federal Court Act* s.10.1.

137 The designated judges could perhaps also consider CSIS warrant requests in order to maintain their experience should terrorism trials involving s.38 issues prove to be rare.

138 It could be argued that existing Federal Court judges with expertise in national security matters should also be allowed to conduct criminal trials. This, however, would require cross-appointing such judges to multiple provincial superior courts.

for managing the difficult and dynamic relationship between secret intelligence and information that must be disclosed to the accused.

7. Abolishing Pre-Trial Appeals

A final reform to make the national security confidentiality process more efficient would be to repeal s.38.09 of the CEA which allows for decisions about national security confidentiality to be appealed to the Federal Court of Appeal with the possibility of a further appeal to the Supreme Court of Canada under s.38.1. The criminal trial process has traditionally avoided appeals of issues before or during a criminal trial because of concerns about fragmenting and delaying criminal trials.

An accused would retain the ability to appeal a non or partial disclosure order as part of an appeal from a conviction to the provincial Court of Appeal as contemplated under the Criminal Code. It could be argued that the provincial Courts of Appeal do not have expertise in matters of national security confidentiality. Provincial Courts of Appeal already hear public interest immunity appeals under s.37 of the CEA. They could take guidance from the s.38 jurisprudence that has been developed and would continue to be developed in the Federal Court in non-criminal matters. Finally, the Supreme Court of Canada maintains the ultimate ability to interpret s.38 for all courts. If pre-trial appeals were abolished under s.38, most appeals would involve many matters of criminal law, procedure and evidence that are within the expertise of the provincial Courts of Appeal in addition to the s.38 issue.

The Attorney General of Canada would lose the right to appeal an order authorizing disclosure, a right that it exercised with partial success in *Khawaja*.[139] It could be argued that this might prematurely sacrifice prosecutions by not allowing the Attorney General an opportunity to establish that a judge had committed legal error and ordered too much information disclosed to the accused. Nevertheless, the Attorney General of Canada would retain the right to issue a certificate prohibiting disclosure under s.38.13 of the CEA or of taking over a terrorism prosecution and entering a stay of proceedings should it conclude that the public interest would be seriously harmed by disclosure. The abolition of pre-trial appeals may require closer co-ordination between the Attorney General of Canada and those who handle terrorism prosecutions either in the provinces or

139 2007 FCA 342. Note however that the error in that case might have been corrected by asking the judge to reconsider his original decision. ibid at paras 18, 52.

through the new federal Director of Public Prosecutions. In any event, there is a need to co-ordinate these processes and the Attorney General of Canada retains the ability to prosecute terrorism offences.[140]
If pre-trial appeals from a s.38 determination are to be retained, however, thought should be given to providing time-limits not only for the filing of appeals, but also for the hearing of arguments and the rendering of decisions.

F) Conclusion

There is an urgent need to reform the process through which national security confidentiality claims are decided. Most of Canada's past terrorism prosecutions have involved material supplied by Canadian and foreign security intelligence agencies and this trend will likely increase given the nature of international terrorism. Although some front-end reforms may make intelligence agencies more willing to disclose intelligence or even to use intelligence as evidence, some secrecy claims will be necessary to protect vulnerable informants, sources and methods and to respect restrictions on the subsequent disclosure of information.

Although there may be some benefits in codifying disclosure and production requirements, and in attempting to define material that clearly does not have to be disclosed or produced, there is a danger that restrictive disclosure and production requirements will generate Charter challenges and increased litigation over the adequacy of disclosure. It may be wiser to improve the efficiency of the process through which the government can seek orders to prohibit disclosure in specific instances. The 2006 MOU between the RCMP and CSIS contemplates the use of s.38 of the CEA to protect CSIS material. Unfortunately, the use of s.38 can threaten the viability of terrorism prosecutions through delay, pre-trial appeals and through non-disclosure orders by the Federal Court that may require a trial court to stay proceedings.

The parties to the Malik and Bagri prosecution took extraordinary and creative steps to avoid litigating issues under s.38. Such litigation in the Federal Court would have delayed and fractured a criminal trial which was already one of the longest and most expensive in Canadian history. If s.38 had been used in the Malik and Bagri prosecution, it is possible that the prosecution would have collapsed or that a stay of proceedings would have been entered under s.38.14. Proceedings also could have

140 *Security Offences Act* R.S. 1985 c.S-7, s.2; *Criminal Code* s.83.25.

been stayed because of CSIS's failure to retain information that was of potential disclosure and evidential value to the accused. Although Air India was a unique case that hopefully will never be repeated, accused will continue to seek disclosure or production of the work of Canada's security intelligence agencies and information collected by our intelligence agencies may in some cases constitute important evidence in terrorism prosecutions. Front-end reforms designed to make intelligence more usable in terrorism prosecutions and back-end reforms to determine in an efficient and fair manner whether intelligence must be disclosed to the accused are required to respond to the unique and difficult challenges of terrorism prosecutions.

The trial judge should be empowered to make decisions about whether secret information needs to be disclosed to the accused. Such an approach should allow the trial judge to make disclosure and national security confidentiality decisions without the inefficiencies and potential unfairness revealed by separate Federal Court proceedings in the *Kevork, Ribic* and *Khawaja* prosecutions. The judge could decide in cases where the intelligence would not assist the accused that disclosure of the secret information was not necessary while retaining the ability to re-visit that decision if necessary to protect the accused's right to make full answer and defence as the trial evolves. Combined with front-end reforms that prepare intelligence to the extent possible for disclosure and use as evidence, a one court approach would move Canada towards the approaches used in other democracies with more experience in terrorism prosecutions. It would provide a better foundation for management of the difficult and dynamic relationship between secret intelligence about terrorist threats and evidence and information that must be disclosed in terrorist trials.

Without significant reforms, there is a danger that terrorism prosecutions in Canada may collapse and become impossible under the weight of our unique two court approach to reconciling the need for secrecy and the need for disclosure and our old habits of ignoring the evidentiary implications of the gathering of intelligence. An inability to try terrorism prosecutions on their merits will fail both the accused and the victims of terrorism.

Kent Roach is a Professor of Law with cross appointments in criminology and political science. He holds the Prichard and Wilson Chair of Law and Public Policy at the University of Toronto. In 2002, he was elected a Fellow of the Royal Society of Canada by his fellow academics. He was a former clerk for the last Justice Bertha Wilson of the Supreme Court of Canada. He has been the editor in chief of the Criminal Law Quarterly since 1998 and has appeared frequently as counsel for various interveners in the Supreme Court and Courts of Appeal. He is the author of nine books including *Constitutional Remedies in Canada* winner of the 1997 Owen Prize for best Canadian law book and (with R.J. Sharpe) *Brian Dickson: A Judge's Journey* winner of the 2004 Dafoe Prize for a book that contributes most to the understanding of Canada. Two other of his books have been shortlisted for the Donner Prize for best public policy work.

In recent years, Professor Roach has focused much of his work on anti-terrorism law and policy. He is the co-editor of *Global Anti-Terrorism Law and Policy* (Cambridge: Cambridge University Press, 2005) and *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill* (Toronto: University of Toronto Press, 2001). He is also the author of *September 11: Consequences for Canada* (Montreal: McGill-Queens Press, 2003) and numerous other articles on anti-terrorism law including the 2002 McGill Law Journal Lecture and the 2005 Viscount Bennett Lecture. These lectures were subsequently published in the McGill Law Journal and the Cardozo Law Review respectively. He has appeared before committees of the Canadian Parliament, Indonesia and the United States Congress on matters related to anti-terrorism law and policy. He was also part of a legal expert group for the United Nation's Office on Drug and Crime that examined penal provisions to implement the Convention for the Suppression of Nuclear Terrorism.

Professor Roach's articles on anti-terrorism laws have been published in Australia, Canada, Egypt, Hong Kong, the Netherlands, Italy, Singapore, South Africa, the United Kingdom and the United States and have also been translated into Arabic, Chinese and Russian. He has lectured on anti-terrorism law and policy at the University of Cape Town, the University of New South Wales, the National University of Singapore, Oxford and Yale. He was a member of the five person research advisory panel for the Commission of Inquiry into the actions of Canadian Officials in Relation to Maher Arar and research director for Ontario's Inquiry into Forensic Pediatric Pathology. He served as Director of Research (Legal Studies) for the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182.