The opinions expressed in these academic studies are those of the authors; they do not necessarily represent the views of the Commissioner.

Cat. No: CP32-89/5-2010E
ISBN: 978-0-660-19984-9

Available through your local bookseller or through
Publishing and Depository Services
Public Works and Government Services Canada
Ottawa, Ontario
KIA OS5

Telephone: (613) 941-5995 or 1 800 635-7943
Fax: (613) 954-5779 or 1 800 565-7757
publications@pwgsc.gc.ca
Internet: www.publications.gc.ca

The Unique Challenges of Terrorism Prosecutions:

Towards a Workable Relation Between Intelligence and Evidence

Kent Roach

Table of Contents

The Unique Challenges of Terrorism Prosecutions: Towards a Workable Relation between Intelligence and Evidence

Kent Roach*

Introduction

The Commission of Inquiry Into the Investigation of the Bombing of Air India Flight 182 has been asked to examine "the manner in which the Canadian government should address the challenge, as revealed by the investigation and prosecutions in the Air India matter, of establishing a reliable and workable relationship between security intelligence and evidence that can be used in a criminal trial" and "whether the unique challenges presented by the prosecution of terrorism cases, as revealed by the prosecutions in the Air India matter, are adequately addressed by existing practices or legislation and, if not, the changes in practice or legislation that are required to address these challenges…"[1] This study, along with companion papers on structural and mega-trial aspects of terrorist trials,[2] and the American experience with terrorism prosecutions[3], is designed to provide background for the Commission's deliberations about how the many challenges presented by terrorism prosecutions may best be faced in the future.

The focus in this study will be on the unique challenges presented by terrorism prosecutions, 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. Most of the unique problems of terrorism trials can be related to the difficulties of establishing a workable and reliable relationship between security intelligence and evidence that can be used in a criminal trial. The relation between intelligence and evidence inevitably implicates the relationship between security intelligence agencies and the police. Ultimately, there is an obligation to reconcile the need for secrecy with the need for disclosure. Legitimate needs for secrecy relate to intelligence sources, investigations, and restrictions or caveats placed

---

* Professor of Law, University of Toronto. Opinions expressed in this paper 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. A summary of this study is available in vol 3 of the Research Studies of the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182.

1 Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 Terms of Reference May 1, 2006. b iii and vi.

2 Bruce MacFarlane Q.C. "Structural Aspects of Terrorist Trials" in Vol. 3 of the Research Studies

3 Robert Chesney "The American Experience with Terrorism Prosecutions" in Vol. 3 of the Research Studies.

on the use of intelligence by third parties. Legitimate needs for disclosure relate to the accused's rights to disclosure and full answer and defence and the public's right to a fair and public trial.

Security intelligence refers to information prepared by various agencies of the government, such as the Canadian Security Intelligence Service (CSIS) and foreign agencies, from closed and open sources about various risks to the national security of Canada. Security intelligence is generally secret and meant to alert officials to risks to national security in order to enable them to take effective preventive measures. Intelligence, for example, led to increased, but ultimately unsuccessful, precautions being taken in 1985 to protect Air India planes originating from Canada. Security intelligence is not collected with a view to its admissibility as evidence in court as proof of wrongdoing or its disclosure to the accused. Security intelligence may be based on hearsay reports of what some people have reported that they have heard others say. Security intelligence may also reveal highly sensitive and confidential methods and sources of covert intelligence gathering and other information that, if released, could harm Canada's national security or defence interests or its relations with other countries. Finally, security intelligence may be collected by methods that may not satisfy constitutional or common law standards that apply to the collection of evidence.

In contrast, evidence is collected by the police in the hope that it will result in the laying of charges and the transmission of evidence to prosecutors. Prosecutors have a duty to disclose relevant information to the accused, and to present evidence in open court in an attempt to prove beyond a reasonable doubt that the accused is guilty of a specific offence. Evidence is collected in accordance with various legal and constitutional standards, and the manner in which evidence is collected may become a subject of litigation as part of the trial process. Evidence is designed to be presented in court, where it will be subjected to adversarial challenge. Subject to certain limited exceptions such as the evidentiary privilege protecting police informers, the police assemble their files and evidence knowing that evidence will eventually be disclosed to the accused and presented in a public criminal trial.

Stated in the abstract, the differences between intelligence and evidence are stark. At the same time, the relation between intelligence and evidence is dynamic.[4] Crimes related to terrorism often revolve around behaviour

4 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.

that may also be the legitimate object of the collection of security intelligence. Even before the enactment of the *Anti-Terrorism Act,* terrorism prosecutions could involve allegations of conspiracies or agreements to commit crimes or other forms of before-the-fact liability. The CSIS mandate has from the start included counter-terrorism investigations, and CSIS was created in the wake of high profile terrorist attacks -- including the October Crisis. 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.

The differences between security intelligence and admissible evidence present several challenges for terrorism prosecutions. A basic, and largely unexplored, question is whether security intelligence can be admitted as evidence in a criminal trial. This question involves the different standards that are used to obtain security intelligence and evidence under the Criminal Code.[5] The Air India investigation raises questions about whether electronic surveillance obtained by CSIS could be admitted as evidence in a criminal trial. The possible admission of such intelligence as evidence also implicates issues of retention of intelligence and disclosure of intelligence to the accused.

Part of the value of security intelligence, especially intelligence based on vulnerable human sources, secret operations and information obtained from foreign agencies, is that it is kept confidential and is used by the government on a need-to-know basis. On the other hand, with respect to evidence to be used at a criminal trial and other relevant information, there are strong presumptions, backed up by the Canadian Charter of Rights and Freedoms, that it should be made public and disclosed to the accused in order to treat the accused fairly and to honour the open court principle. The constitutional disclosure obligations of the Crown to the accused go significantly beyond disclosing evidence to be used in the criminal trial to including other non-privileged information that is relevant to the case.[6] The courts have also held that information used to obtain warrants should be disclosed to the accused in order to allow the accused to challenge the warrant. [7] Even if security intelligence is not held, as it was in the *Malik and Bagri* trial, to be subject to disclosure

5 R.S.C. 1985 c.C-34 Part VI.
6 *R. v. Stinchcombe* [1991] 3 S.C.R. 326.
7 See *R. v. Parmar* (1987) 31 C.R.R. 256 and *R. v. Atwal* (1987) 36 C.C.C.(3d) 161 case studies discussed infra section 3.

obligations, the courts have recognized that the accused should have access to information held by third parties. [8]

Disclosure to the accused and the public is supported by the Charter, but it is not an absolute value. The Court has drawn a distinction between broad rights of disclosure under s.7 of the Charter and more limited principles that revolve around being able to know the case to meet and to make full answer and defence.[9] Sections 37 and 38 of the *Canada Evidence Act* (CEA) provide procedures that allow the Attorney General of Canada (AG) to apply to courts to obtain orders for non-disclosure or modified disclosure of sensitive material. The Attorney General of Canada has a power under s.38.13 of the CEA to prevent even court-ordered disclosure of material received from foreign governments or disclosure of material that relates to national security or national defence. The discussion, in this paper, of the proper relation between security intelligence and evidence will require consideration of the accused's Charter rights to disclosure and full answer and defence, the open court principle protected under the Charter and the procedures that are available to maintain the confidentiality of security intelligence from disclosure to the accused and the public.

The importance and the difficulty of the many different issues raised by the relation between security intelligence and evidence cannot be underestimated. Taken together, they raise fundamental issues about the viability of criminal prosecutions for terrorism as well as about the important role of security intelligence that flows within and between governments. Both the law and the nature of intelligence should evolve to reflect the dangers of terrorism and the competing demands of secrecy and disclosure.

The relation between evidence and intelligence is dynamic. Our thinking about keeping secrets should evolve beyond a Cold War paradigm in which counter-intelligence dominated the work of security agencies and secrets about the enemy could be kept perhaps forever. 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 at which it is imperative to arrest and prosecute people. They must resist the

---

8 *R. v. O'Connor* [1995] 4 S.C.R. 401.

9 *R. v. Dixon* [1998] 1 S.C.R. 244*; R. v. Taillefer* [2003] 3 S.C.R. 307. On the importance of knowing the case to meet in the immigration context see *Charkaoui v. Canada* 2007 SCC 9.

temptation to engage in over-classification and unnecessary claims of secrecy. That said, the criminal process must also evolve to take account of the particular challenges of terrorism prosecutions. There is a need for efficient and fair means to require that only truly relevant information necessary for a fair trial must be disclosed to the accused. There must be an efficient and practical venue for the state to assert its interest in national security confidentiality. Both the intelligence and legal sides of the equation must change to respond to the challenges of international terrorism of which the 1985 Air India bombing was a horrific precursor.

Intelligence can be kept secret if it is only used to inform government of threats to national security.[10] 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. 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.[11] Canada must make every effort to avoid miscarriages of justice in the future. 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 be placed in the unnecessary and impossible position of choosing between disclosing information that should be kept secret to protect sources, operations and foreign confidences or declining to bring terrorism prosecutions. This most difficult choice should only be necessary in cases where a fair trial is not possible without disclosure.

The choice between disclosure and prosecution is not a matter of hypothetical theory. 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

---

10 The Commission of Inquiry into the Activities of Canadian Officials in Relation to Maher Arar has, however, stressed the need for review bodies to have access to secret material. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar *A New Review Mechanism for the National Security Activities of the RCMP* (Ottawa: Supply and Services, 2006).

11 Bruce MacFarlane "Structural Aspects of Terrorist Trials" in Vol 3 of the Research Studies; Kent Roach and Gary Trotter "Miscarriages of Justice in the War Against Terrorism" (2005) 109 Penn. State Law Review 1001.

been the mastermind of the bombing of Flight 182. The other involved a conspiracy to blow up another Air India plane in 1986.[12] Although the Air India trial of Malik and Bagri did go to verdict in 2005, it could also have collapsed over issues of whether or not 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.[13] In addition, the trial judge did not have to order a remedy for the destruction of both wiretaps and notes by CSIS that should have been retained and disclosed to the accused only because he acquitted the accused.[14] Other prosecutions in Canada, including the first prosecution under the 2001 *Anti-Terrorism Act* (ATA)[15], have experienced difficulties and delay as a result of proceedings taken to obtain orders that intelligence or other secret information not be disclosed to the accused. 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. Both intelligence agencies and the justice system need to adjust to the challenges of terrorism prosecutions.

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, however, the justice system should ensure that the secret information is truly necessary for a just 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 which 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 concerns about national security confidentiality, even if these concerns are legitimate.

The search for reasonable alternatives which can reconcile the demands of fairness and secrecy is not limited to the formal processes of the justice

---

12 *R. v. Parmar* (1987) 31 C.R.R. 256 discussed infra section 3; *R. v. Khela* [1996] Q.J. no. 1940 discussed infra section 5.

13 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).

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

15 *Canada. v. Khawaja* 2007 FC 463; *Canada. v. Khawaja* 2007 FC 490; *Canada. v. Khawaja* 2007 FCA 342; *Canada. v. Khawaja* 2007 FCA 388; *Canada v. Khawaja* 2008 FC 560 discussed infra section 6.

system. Efforts must be made to convince confidential informers that their identity can be revealed and that they will be protected through witness 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 treatment of confidential sources and the recording of surveillance and interviews, 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.[16] It does mean that CSIS should be aware of the evidential and disclosure demands of terrorism prosecutions. Reconciling the contradictory demands of fairness and secrecy is one of the most difficult and delicate tasks faced by prosecutors, security agencies, judges and society alike. It is also one of the most important tasks to accomplish 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 historical outline of thinking about the distinction between security 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, for it to be 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 respective roles of police and security intelligence agencies are grounded in principle and statute. At the same time, however, they are not set in stone and they continue to evolve. The distinction between proactive intelligence and reactive law enforcement that was conventional wisdom in 1984 may no longer be acceptable today. Any contemporary discussion of the distinction between security intelligence and evidence should account for the enactment of the *Anti-Terrorism Act* in 2001. This act was designed to give the police more tools to prevent terrorism before it happens: primarily through prosecutions of various crimes for financing, support, and preparation for terrorism.

---

16 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.

The second part of this paper will outline some of the competing goals that should inform the relationship between security intelligence and evidence. These include: 1) the need to respect the confidential and highly sensitive nature of intelligence including methods, sources, ongoing investigations and information received from third parties; 2) the need to treat the accused fairly under the Charter especially with respect to the right to full answer and defence; 3) the need to respect the presumption that courts will be open to the public and the press; and 4) the need to ensure that criminal courts can efficiently and accurately reach verdicts in terrorism trials. Ultimately, there is a need to reconcile the need for secrecy with the need for disclosure.

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 the state may want to use intelligence as evidence in terrorism trials. This raises the issue of whether information collected by CSIS, including information from CSIS wiretaps, as well as intercepts collected under ministerial authorization by the Communications Security Establishment (CSE), 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 maintaining the appropriate balance between CSIS and Criminal Code warrants, will be examined in the third part of this paper.

In order to focus discussion, relevant case studies will be used throughout this paper. In this third part, the case studies will include the abandoned prosecution against Talwinder Singh Parmar, and others, in relation to an alleged Hamilton plot to commit acts of terrorism in India, after the accused successfully sought access to an affidavit used to obtain a Criminal Code authorization to engage in electronic surveillance. The second case study examined in this part will be the Atwal case, involving attempted murder convictions and abandoned conspiracy to commit murder charges in relation to the shooting of Indian Cabinet minister Malkiat Singh Sindu. *Atwal* remains the leading case with respect to the admissibility of CSIS wiretaps as evidence in criminal trials.

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 retain and 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 disclosed and produced under the procedure that applies under *O'Connor* 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 limit *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 privilege, as well as Charter challenges.Throughout this analysis, I will draw on the relevant experience, as revealed by the Air India prosecution, as well as other terrorism prosecutions, such as the *R. v. Khela* case, in which a stay of proceedings was eventually entered after the Crown failed for many years to reveal the identity of, and statements taken from, a key informant who participated in the discussions leading to the conspiracy charges with respect to an alleged plan to bomb another Air India plane in 1986.

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,* as amended by the 2001 ATA. 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: 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. Although the s.38 procedure was not used in the Air India trial, it could have been used had prosecuting and defence counsel not been able to fashion an alternative regime of disclosure, subject to an initial undertaking that defence lawyers not disclose the evidence to their clients. The limited use of s.38 in terrorism prosecutions will be examined in the *Kevork* and *Khawaja* cases, as will its use in the *R. v. Ribic* prosecution relating to a hostage taking in Bosnia.

The seventh part of this paper will examine the procedures used in the United States, the United Kingdom and Australia to resolve claims of national security confidentiality, with a view to understanding how the approaches used in those countries differ from those used in Canada and whether they provide a sounder basis for maintaining a workable and reliable relationship between security intelligence and evidence. A striking feature of these comparative regimes is that they all allow a criminal trial court to resolve and revisit claims of national security confidentiality and consequent non or partial disclosure orders in light of the evolving nature of the criminal prosecution. In contrast, the Canadian approach contemplates the Federal Court making final and binding orders with respect to non-disclosure and the criminal trial court then deciding whether a fair trial is still possible in light of the Federal Court's non-disclosure orders.

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 the 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 evidential 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 by intelligence agencies.

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 evidential privileges; 3) providing a means by which secret material used to support 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.

All of these issues are united by the need to establish a reliable, workable and fair relationship between intelligence and evidence. They raise fundamental questions about the viability of criminal prosecutions as a response to the threats of, and to acts of, international terrorism such as that which resulted in the bombing of Air India Flight 182.

I. The Evolving Distinction Between Security Intelligence and Evidence

In this section, I will examine public thinking about the perceived difference between security intelligence and evidence and its relation to the distinct roles played by security intelligence agencies and police forces. I will take an historical approach in order to trace the evolution of thinking about the differences between security intelligence and evidence as we moved from a Cold World era that emphasized counter-intelligence against a hostile state, to a post 9/11 world, where the emphasis is on counter-terrorism against hostile non-state actors. The 1985 Air India bombing has a particular significance in this evolution. It was a tragic and horrific foreshadowing of the post 9/11 era. At the same time, it is not clear that our thinking about the relation between intelligence and evidence has evolved sufficiently to reflect the threat of terrorism or the need to prosecute terrorists.

A) The Mackenzie Commission

The first Canadian recommendation that the collection of security intelligence be separated from policing was made in 1969 by a Royal Commission on Security, commonly called the MacKenzie Commission after its chair. This Commission examined a number of different topics such as security clearances, immigration and security and external affairs and industrial security; none of which were focused on law enforcement. The Commission explained that the security procedures that it would examine:

> …are not necessarily related to the detection and prosecution of illegalities, where precise legal definitions would be of central importance, but are mainly concerned with the collection of information and intelligence, with the prevention and detection of leakages of information and with prevention against attempts at subversion.[17]

It proposed the creation of a civilian intelligence agency with a preventive mandate that would be distinct from the more reactive law enforcement mandate of the police.

---

17 *Report of the Royal Commission on Security* (Abridged) (Ottawa: Information Canada, 1969) at para 4.

The Mackenzie Commission proposed that wiretapping for security reasons be exempted from proposed legislation enforcing the provision of judicial warrants, and that it be be subject to Ministerial authorization. It concluded that "ministers are more readily aware of the full details of the cases brought to their attention, are in a better position to understand the special requirements of security, and could maintain more centralized control of the complete range of wiretapping operations."[18] It recognized that the new security intelligence agency "should, when necessary, operate in close liaison and co-operation with the RCMP and other police forces"[19], but it did not deal with the difficulties of managing the relation between intelligence and evidence.

B) The McDonald Commission

The McDonald Commission examined RCMP activities, including unlawful activities, that were committed in the wake of the 1970 October Crisis, in which two terrorist cells in Quebec committed a kidnapping and a murder. It observed that some illegal acts were committed by the RCMP because "a feeling developed that, because the law could be applied only after offences were committed, the enforcement of the law was an inadequate means of effectively forestalling politically motivated acts of violence."[20]

The Commission recommended the creation of a civilian security intelligence agency that could investigate various threats to the security of Canada, including terrorism. The Commission defined security intelligence as "advance warning and advice about activities which threaten the internal security of Canada".[21] With respect to terrorism, the Commission observed:

> Acts of political terrorism, when there is reason to believe they are about to occur or after they occur, are properly the concern of law enforcement agencies. But governments and police forces in Canada should have advance intelligence. Immigration authorities, for example, should have information about international

18 Ibid at para 292.
19 Ibid at para 297
20 Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police *Freedom and Security under the Law* (Ottawa: Ministry of Supply and Services, 1981) at 269.
21 Ibid at 414.

> terrorists to be able to identify them when they apply for entry to Canada….Canada, as a signatory to several international conventions concerning international co-operation in combating terrorism…is obliged to contribute to the international pool of intelligence about terrorists[22]

The Commission stressed that security intelligence was the product both of information collected, often through covert investigations, and of "an analysis of the information based on an assessment of its significance in both a national and international context."[23] It concluded that the security intelligence function should be located outside of the RCMP because of the need for political judgment and direction of security intelligence work and because of the dangers of combining police powers with the collection of security intelligence.[24] The McDonald Commission was more aware of terrorism than the Mackenzie Commission, which it noted had not even mentioned the word terrorism,[25] and it contemplated that the RCMP would play a continuing role in the investigation of offences relating to national security, including apprehended and actual acts of terrorism. Nevertheless, the McDonald Commission's focus was not on the relationship that would emerge between a new civilian security agency and the police[26] or the relation between intelligence and evidence.

C) The Pitfield Committee

In 1983, a Special Senate Committee known as the Pitfield Committee after its chair, Senator Michael Pitfield, examined the distinction between intelligence and evidence at some length and in terms that continue to be influential. The Pitfield Committee 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

22 ibid at 416
23 ibid at 419
24 ibid at 423, 614
25 ibid at 40
26 The McDonald Commission's examination of the police focused on matters such as complaints, legal advice, police powers and the police's relation with the Solicitor General. Ibid at 957-1053.

> not necessarily concerned with breaches of the law. Considerable publicity accompanies and is an essential part of the enforcement of the law. Security intelligence work requires secrecy. Law enforcement is 'result-oriented', emphasizing apprehension and adjudication, and the players in the system- police, prosecutors, defence counsel, and the judiciary- operate with a high degree of autonomy. Security intelligence is, in contrast, 'information-oriented'. Participants have a much less clearly defined role, and direction and control within a hierarchical structure are vital. Finally, law enforcement is a virtually 'closed' system with finite limits- commission, detection, apprehension, adjudication. Security intelligence operations are much more open-ended. The emphasis is on investigation, analysis, and the formulation of intelligence.[27]

The observations of the Pitfield Committee represent influential but flawed thinking about the distinction between law enforcement and intelligence at the time of the creation of CSIS, and this flawed thinking was also evident during the initial Air India investigation. Law enforcement was defined in narrowly reactive terms. Police and prosecutors were autonomous actors that entered the scene after a crime has been committed. The police independently collected evidence to be introduced in a public trial while security intelligence agencies subject to political direction proactively collected advance information about threats. The distinctions between intelligence and evidence collection could not have been stated more starkly. The proactive role of the police in preventing crime and in prosecuting attempts and conspiracies to commit acts of terrorism was ignored. Not surprisingly, the possibility that intelligence could have evidential value in a criminal trial was also ignored.

D) The 1984 CSIS Act and the Security Offences Act

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

---

27 *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.

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.[28]

CSIS was created in a manner that allowed political direction and review and oversight of the new agency in a manner different from the norms that governed the relations between the police and the government. [29] CSIS can be tasked by the Minister of Defence and Minister of Foreign Affairs to provide information and intelligence in certain circumstances.[30] Section 12 of the *CSIS Act* contemplated that CSIS would collect information and intelligence about threats to the security of Canada under standards that differed from those used by the police. It provides that "the Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada." The act specifically refers to information and intelligence as distinct from evidence and it predicates investigations on reasonable grounds of suspicion of threats to the security of Canada.

The *CSIS Act* provided for a separate warrant regime that specifically excluded the existing scheme under Part VI of the Criminal Code[31]. A CSIS wiretap warrant required reasonable grounds to conclude that electronic surveillance was required to investigate a threat to the security of Canada or to investigate foreign states or persons in matters in relation to the defence of Canada and the conduct of its international affairs, as opposed to reasonable grounds to believe that a crime had been committed and that the surveillance would reveal evidence of the crime.[32] All of these matters distinguished the role of CSIS in providing security intelligence to the government from the role of the police in collecting evidence to justify the laying and prosecution of charges.

---

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

29 On the evolving norms of police independence which stress the legitimate role of transparent Ministerial directives to the police see Commission of Inquiry into the Activities of Canadian Officials in Relation to Maher Arar *A New Review Mechanism for the RCMP's National Security Activities* (2006) ch 9; *Report of the Ipperwash Inquiry Policy Analysis* (2007) ch.12.

30 *CSIS Act* ss.13-16

31 ibid s.26

32 ibid s.21

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"[33]. 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) of the *CSIS Act* provided that 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…"[34] 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 an impermeable wall between intelligence and relevant information to 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 much less noticed companion legislation to the *CSIS Act*, the *Security Offences Act*[35]. 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[36]. A broad range of offences, including murder, attempted murder, other forms of violence or threatening, 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 dichotomy 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

---

33 Ibid s.18.
34 Ibid s.19(2)(a).
35 R.S.C. 1985 c.S-7 s.6.
36 RCMP Act s.18

and prosecutions. It established overlapping jurisdictions by giving CSIS a mandate to investigate acts of terrorism, defined as threats and acts of serious violence directed at persons or property for political ends, that could both before and after completion constitute crimes. The RCMP was given primary jurisdiction over these crimes. Their role was not solely reactive because they had a mandate to prevent crime and they could investigate and lay charges both before and after acts of terrorism.

E) The Distinction Between Evidence and Intelligence in the Post Air India Bombing Period

A July 1984 MOU provided a bare-bones framework for the sharing of information between the RCMP and CSIS. After outlining areas where information could be shared, it provided that "neither CSIS nor the RCMP shall have an unrestricted right of access to the operational records of the other agency" and "shall not initiate action based on the information provided without the concurrence of the other agency." The vague reference to "action" would presumably cover legal proceedings, but it could also cover a broad range of investigative activities. The MOU went on to provide that "operational information" from joint operations of the RCMP and CSIS "shall be freely shared between the two agencies" but with "source and third party information excepted."[37]

A more comprehensive 1986 MOU devoted a chapter to information sharing between the two agencies. It contemplated that a Deputy Director of CSIS and a Deputy Commissioner in the RCMP would "interface" with respect to information sharing, but that "Any disagreement regarding the sharing of information or the action to be taken based on such information not resolved by the Director (CSIS) and the Commissioner (RCMP) shall be referred to the Solicitor General (or his designate) for resolution." The fact that both the RCMP and CSIS were under the direction of the same Minister provided the potential for resolving disputes over information sharing and the subsequent use of information. The Solicitor General, in consultation with Cabinet, could ultimately decide whether it was more important to keep secrets or bring prosecutions.

Unlike the 1984 MOU, the 1986 MOU specifically tracked s.19(2) of the *CSIS Act* by providing that CSIS agreed to provide "information to the RCMP:

---

37 MOU signed July 17, 1984 pub doc RCMP 00001.0352

i. relevant to the investigation and enforcement of alleged security offences or the apprehension thereof which fall under the primary responsibility of the RCMP pursuant to s.6(1) of the Security Offences Act[38]

This provision recognized that both the *CSIS Act* and the *Security Offences Act* contemplated a continued national security role for the RCMP. At the same time, the MOU did not specifically address the treatment of the information provided by CSIS to the RCMP with respect to judicial proceedings. There was no reference to steps that could be taken to protect secret intelligence under the *Canada Evidence Act*.

In 1987, a Special Senate Committee on Terrorism and Public Safety commented on reports alleging a lack of co-operation "between federal police and intelligence-gathering agencies on one hand and (provincial) Crown prosecutors on the other in the prosecution of alleged terrorists." It stated that there was "at least one instance where provincial Crown prosecutors failed to obtain a judgment against alleged terrorists at least in part due to CSIS' decision not to allow its officers to testify or to disclose certain information."[39] As will be seen in the subsequent parts of this study, a number of terrorism prosecutions had by this time collapsed or been strained over issues of disclosure of CSIS information or disclosure of informants.

The Special Senate Committee concluded that problems in the relation between CSIS and law enforcement bodies were related to a lack of understanding of CSIS's role, which it described as being "essentially intelligence and information gathering for risk assessment" and not as being to "gather evidence to support criminal prosecutions."[40] The Committee concluded that CSIS "should cooperate fully with provincial Crown prosecutors in the prosecution of alleged terrorists, but not to the extent of prejudicing the safety of CSIS officers, their contacts or of important, ongoing investigations."[41] This recommendation was not likely to solve problems or conflicts in the relation between CSIS and law enforcement, given the primacy that CSIS, as well as the *CSIS Act* itself, gave to the protection of the secrecy of its informants, its operations and its officers.

---

38 MOU signed November 1986 Chapter 13.
39 Chair Hon. William Kelly *Terrorism The Report of the Senate Special Committee on Terrorism and Public Safety* (Ottawa: Ministry of Supply and Services, 1987) at 41
40 ibid at 41
41 ibid at 41

A recommendation that did have some potential for resolving conflicts between security intelligence agencies and the police was that the federal Attorney General assert jurisdiction in terrorism prosecutions that might involve CSIS information and witnesses. This recommendation could keep disputes about whether the public interest was best served by secrecy or disclosure within the federal government. Such disputes would involve the Solicitor General, with responsibility for both CSIS and the RCMP, and the Attorney General of Canada, with an independent responsibility to determine whether prosecutions were in the public interest. The assertion of federal preeminence with respect to terrorism prosecutions was contemplated in the *Security Offences Act*. Although it would not solve all the conflicts between disclosure and secrecy, it would keep them all under the same roof.

The 1987 Senate report essentially accepted the stark dichotomy between evidence and intelligence gathering that was reflected in the 1983 Pitfield report. It did not engage in a rethinking of the relation between intelligence and evidence in light of the Air India bombing. Although urging co-operation between the RCMP and CSIS, it maintained the primacy of protecting the confidentiality of CSIS investigations, agents and informers over the need to reveal such information and intelligence when required to do so in a criminal prosecution.

In 1987, the Independent Advisory Team on CSIS also confirmed a sharp distinction between the intelligence gathering and analysis functions of CSIS and the evidence gathering and prosecution functions of the police. In the course of recommending increased efforts towards civilianization and analysis, the Advisory Team summarized the "fundamental differences between security intelligence work and police work" as follows:

- police deal with facts (evidence) usually after the event, whereas security intelligence agencies try to anticipate events;

- police forces must have a degree of independence from Government control, whereas security intelligence agencies require closer control to ensure that individual rights are not unnecessarily infringed, and where they are infringed, to ensure that political accountability exists;

- police activities are subject to an extensive and detailed set of rules (the Criminal Code and jurisprudence), while security intelligence activities, though provided for by the *CSIS Act*, involve greater judgment in their implementation; and finally,

- a security intelligence agency must keep its Government informed of threats to national security, while police work will normally culminate in evidence being laid before a Crown Attorney for presentation to the Court.[42]

The emphasis in this report was on improving CSIS's ability to collect and assess intelligence, and not on its ability to work with the police. Unfortunately, neither this report nor the Senate report of the same year addressed questions that were essential to the ongoing Air India investigation.

In its 1988-89 annual report, SIRC commented on some tensions between various police forces and CSIS. It explained:

> With a mandate to bring criminals to justice, the police have reason to treat all information as potential evidence for production in court. CSIS has a different mandate, to gather information as a basis for advice to government, and is understandably anxious to protect information that could 'burn' a source.[43]

These comments reaffirmed the traditional divide between the police mandate to collect evidence and the security intelligence mandate to collect confidential intelligence. This conventional wisdom was first articulated by the Pitfield Committee in 1983 and it did not appear to change after the 1985 Air India bombing.

In 1988 Addy J. addressed some of the differences between intelligence collected by CSIS and evidence collected for criminal investigations. In upholding the denial of disclosure of CSIS information in the course of a judicial review of a denial of a security clearance, he stated that:

---

42 *People and Process in Transition Report to the Solicitor General by the Independent Advisory Team on* CSIS October 1987 at 5.

43 SIRC Annual Report 1989-1990 at 38.

> the fundamental purpose of and indeed the *raison d'etre* of a national security intelligence investigation is quite different and distinct from one pertaining to criminal law enforcement, where there generally exists a completed offence providing a framework within the perimeters of which investigations must take place and can readily be confined. Their purpose is the obtaining of legally admissible evidence for criminal prosecutions. Security investigations on the other hand are carried out in order to gather information and intelligence and are generally directed towards predicting future events by identifying patterns in both past and present events.
>
> There are few limits upon the kinds of security information, often obtained on a long-term basis, which may prove useful in identifying a threat…An item of information, which by itself might appear to be rather innocuous, will often, when considered with other information, prove extremely useful and even vital in identifying a threat. The very nature and source of the information more often than not renders it completely inadmissible as evidence in any court of law. Some of the information comes from exchanges of information between friendly countries of the western world and the source of method by which it is obtained is seldom revealed by the informing country.
>
> Criminal investigations are generally carried out on a comparatively short-term basis while security investigations are carried out on systemically over a period of years, as long as there is a reasonable suspicion of the existence of activities which could constitute a threat to the security of the nation….
>
> [a]n informed reader may at times, by fitting a piece of apparently innocuous information from the general picture which he has before him, be in a position to arrive at some damaging deductions regarding the investigations of a particular threat or of many other threats to national security….[44]

---

44 *Henrie v. Canada (Security Intelligence Review Committee)* (1988) 53 D.L.R.(4th) 568 at 577-578 affd (1992) 88 D.L.R.(4th) 575 (Fed.C.A.)

Justice Addy argued that secret nature of intelligence, often received "from exchanges of information between friendly countries of the western world", rendered it "completely inadmissible as evidence in any court of law." His comments discounted the possibility that intelligence might have evidential value. As will be seen in a subsequent section, an attempt had already been made by this time to introduce CSIS wiretaps in a terrorism prosecution.[45] Justice Addy also demonstrated a concern about the mosaic effect of disclosing intelligence. The assumption was that "an informed reader", probably intelligence agents of the Soviet Union or its allies, could piece together ongoing operations or sources from "apparently innocuous information." As will be seen, Justice Addy also cited the mosaic effect in a 1984 case involving a terrorism prosecution[46] and ordered that CSIS material not be disclosed to the accused without even examining the material.

A refusal to consider the evidential value of security intelligence may have made some sense during the height of the Cold War. CSIS and its counterparts were primarily concerned with spying by the Soviet Union and its partners. Criminal prosecutions did not play an important role in this work. It did not, however, fit the nature of counter-terrorism work that could result in prosecutions of non-state actors. As the 1980's drew to a close and the Soviet Union and its empire started to collapse, the conventional wisdom about the stark and absolute divide between secret intelligence and public evidence slowly began to be questioned.

F) Initial Recognition of the Problems of Converting Intelligence into Evidence

In 1990, a Special Committee of the House of Commons conducted a five-year review of the *CSIS Act*. This report recognized "the difficulties of serious technical problems to be overcome regarding the process by which intelligence generated by CSIS can be transformed into criminal evidence, especially in cases where politically motivated violence is concerned."[47] The Committee reported complaints from the RCMP that while CSIS passed information to the RCMP, "the information received was often 'too massaged' to be of much real use." The Committee raised concerns, however, about whether raw intelligence would put CSIS sources in jeopardy and "whether evidence obtained directly from CSIS sources and methods can be used successfully in court without a

45 *R. v. Atwal* (1987) 36 C.C.C.(3d) 161 (Fed.C.A.).
46 *Re Kevork* (1984) 17 C.C.C.(3d) 426 (F.C.T.D.) discussed infra Part IV
47 *In Flux But Not in Crisis* at 105

Charter challenge."[48] This raised concerns about different standards for authorizing electronic surveillance under the *CSIS Act* and the Criminal Code that will be discussed more fully in part 3 of this study, as well as concerns about the disclosure of CSIS informants and/ or officers that might be required in criminal prosecutions. Having identified some of the difficulties of converting intelligence into evidence that could be admitted and disclosed in terrorism prosecutions, however, the five year review Commons committee did not propose any solutions for addressing them.

A new MOU signed between the RCMP and the CSIS in 1990 also demonstrated increased awareness of the difficulties of managing the relation between secret intelligence and public evidence. Section 7 of this MOU provided:

> The CSIS and the RCMP recognize that from time to time information and intelligence provided by the CSIS to the RCMP will have potential value as evidence in the investigation or prosecution of a criminal offence. Both parties further recognize that, given that CSIS does not normally collect information for evidentiary purposes, such use is exceptional and will not be considered without the prior approval of CSIS. When such use is taken, full account will be taken of the balance of public interest in the particular case, including the seriousness of the crime, the importance and uniqueness of the information provided by the CSIS, and the potential effects of disclosure on CSIS sources of information, methods of operations and third party relations.

This provision recognizes that, in "exceptional cases", intelligence could be used as evidence and helpfully provided some public interest criteria to guide such decisions. The criteria speak both to the need and importance of the evidence in the particular case as well as the harm that the use of the evidence may cause to CSIS operations and third party relations.

Section 9 of the 1990 MOU also provided that pursuant to s.19(2)(a) of the *CSIS Act,* which contemplates CSIS provision of information to be used by the police in their investigations or prosecutions, that "CSIS agrees to provide 'spin-off' information and intelligence to the RCMP" relevant to

---

48 ibid at 104

the investigation of indictable offences where the RCMP had jurisdiction over the offence. The meaning of 'spin-off' information and intelligence is not clear, but it seems to contemplate that primary information and intelligence collected by CSIS may not necessarily be disclosed. The MOU recognized that intelligence would be used in criminal prosecution, but only in "exceptional cases" and only as a "spin-off" from CSIS's mandate to collect secret intelligence to inform the government about threats to national security.

Finally, section 24 of the MOU provided that in addition to respect for caveats and the confidentiality of information that:

> Subject only to the requirements of the Courts, information provided by either party to this Memorandum of Understanding shall not be used for the purpose of obtaining search warrants or authorizations to intercept private communications, produced as evidence in Court proceedings or disclosed to Crown Prosecutors or any third-party without the prior express approval of the party that provided the information.
>
> Nothing in this Memorandum of Understanding shall be interpreted as compelling either party to disclose the identity of its sources or caveated information from a third party.[49]

This provision required CSIS or the RCMP to consent to information being used to obtain judicial warrants. This recognized that information used to obtain a judicial warrant would be subject to disclosure requirements in order to allow the accused to challenge the legality of the warrant. By that time, both the police and CSIS had experience with the disclosure of the information used to obtain both Criminal Code and CSIS wiretaps in terrorism investigations.[50]

The 1990 MOU also required CSIS consent before such information was disclosed to prosecutors or used in court. As will be discussed in the fourth part of this study, however, the Supreme Court constitutionalized a broad right to disclosure in *Stinchcombe* in 1991; a year after the MOU was signed. Although information held by Crown prosecutors was

---

49 MOU signed August 21, 1989 pub doc RCMP 0001.0352

50 See the discussion of *R. v. Parmar* and *Atwal v. Canada* in Part 3 of this study.

subject to disclosure obligations, *Stinchcombe* in effect required full disclosure of relevant and non-privileged information held by the police about a case, whereas the MOU contemplated CSIS having a veto over whether information it disclosed to the police would in turn be disclosed to the prosecutor for possible disclosure to the accused. The 1990 MOU was catching up to the difficulties of managing the relation between intelligence and evidence, but its emphasis on secrecy and CSIS consent for the disclosure of information were still in tension with evolving disclosure requirements.

G) SIRC Reports on the Air India Investigation and RCMP/CSIS Co-Operation

The SIRC report on the bombing of Air India also considered matters related to the distinction between security intelligence and evidence. SIRC reported that CSIS officials had notified the RCMP about what they believed to be a one shot discharge of a rifle that was heard during the surveillance of Parmar and Reyat at Duncan. This was consistent with s.19(2) of the *CSIS Act* which contemplated that CSIS could transmit information that might be relevant to a criminal investigation to the police. In the aftermath of the bombing, SIRC expressed some concern that the senior management of CSIS did not clarify CSIS's mandate in relation to the RCMP or "set out CSIS policy on the sharing of information and intelligence with the RCMP."[51] Despite the lack of policies regarding the sharing of information with the RCMP, SIRC related the post-bombing difficulties between the two agencies to differences of mandate. It stated:

> As the investigation progressed, RCMP officials felt it necessary to examine certain CSIS files on certain Sikh extremist targets in more detail. *CSIS, whose mandate is to collect intelligence and not evidence, was at first reluctant to expose its files, and by extension its methods and sources, for any evidentiary use by the RCMP*. Lengthy negotiations took place between the two agencies, but eventually the RCMP investigators were allowed access to the files subject to some mutually agreed upon conditions on the subsequent use of the information.

---

51 Security Intelligence Review Committee Annual Report 1991-1992 (1992) at 10.

> Overall, we found no evidence that access to CSIS information relevant to the RCMP investigation of the disaster was unreasonably denied to the Force.[52]

SIRC also relied on its understanding of the CSIS mandate when evaluating CSIS's erasure of tapes of Parmar's electronic surveillance. Although criticizing the lack of clarity about CSIS's retention policy, it commented that an instruction "which removed from Service facilities the capacity to collect and preserve criminal evidence tapes" was "consistent with the provisions of the *CSIS Act* establishing the Service as an intelligence agency with no police powers or responsibilities."[53] Although the problems of converting intelligence into evidence had been identified by the five-year Parliamentary review committee, and in the 1990 MOU between the RCMP and CSIS, efforts to overcome these difficulties were countered by assumptions which relied on the different mandates of the RCMP and CSIS, and by the notion that intelligence would only be used in prosecutions in exceptional cases.

In 1998 and 1999, SIRC conducted a study of RCMP/CSIS relations. It noted that previous "difficulties and disagreements appear to centre mainly, but not entirely, on the exchange of information and intelligence between the RCMP and CSIS on operational matters and thus, if widespread or systemic, could affect cooperation at its most fundamental level."[54] This report outlined a system in which RCMP liaison officers at CSIS had access to much information, but to which caveats restricting the subsequent use of the information were generally attached. Even advisory letters from CSIS that contemplated the use of information to obtain a search warrant reserved the right of CSIS to challenge by any means the release of CSIS information without consultation and approval from CSIS.[55] SIRC commented:

> 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

---

52 ibid at 10 (italics added)
53 ibid at 11
54 CSIS Co-operation with the RCMP Part 1 (SIRC Study 1998-04) 16 October, 1998 at p.2.
55 ibid at 8.

> 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. [56]

In this passage, SIRC expressed concerns that CSIS information might not be admitted into criminal trials because it was not collected to evidentiary standards and that the use of ss.37 and 38 of the Canada Evidence Act to protect CSIS information from disclosure could threaten criminal prosecutions. As will be seen, these are serious and legitimate concerns. Nevertheless, they are concerns mainly for the prosecution. They should only affect CSIS to the extent that CSIS might be asked to alter its practices in some cases in order to collect information, such as physical surveillance, to evidentiary standards or to support the RCMP in obtaining Criminal Code search warrants. The root of the problem, as SIRC correctly noted, was not so much the difficulties in using intelligence in criminal prosecutions, though these might be considerable, but rather CSIS's unwillingness to expose its investigations, sources and officers to disclosure. The reluctance of CSIS to risk such disclosure had support in its mandate to collect secret intelligence and, in the offences in s.18 of the *CSIS Act*, to disclose confidential sources and covert operations. Nevertheless, any global defence of secrecy begged the question of whether in a particular case, prosecution and disclosure was in the public interest.

SIRC also 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 appended the full text of the decision to its report and commented that:

> The impact of that decision is that all CSIS intelligence disclosures, regardless of whether they would be entered

---

56 ibid at 9.

> for evidentiary purposes by the Crown, are subject to disclosure to the Courts. Any passage of information, whether an oral disclosure or in a formal advisory letter, could expose CSIS investigations. This means that even information that is provided during joint discussions on investigations or that is provided as an investigative lead is at risk.[57]

This was a very expansive and somewhat alarmist reading of the implications of *Stinchcombe*. 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 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. [58]

SIRC raised concerns about the decentralized nature of the RCMP that led to different interpretations of *Stinchcombe* disclosure obligations.[59] It may have been helpful in such circumstances to have gotten some consensus about the precise extent of disclosure obligations rather than to have assumed that they were very broad. SIRC's argument that *Stinchcombe* had made relations between CSIS and the RCMP worse also downplayed difficulties that had arisen in the relationship long before the Supreme Court's 1991 decision. A case in point that will be subsequently examined is the 1987 decision in *Atwal* that had led to the disclosure of information used to obtain a CSIS electronic surveillance warrant and the eventual resignation of the director of CSIS because of inaccuracies in that affidavit. Long before *Stinchcombe*, CSIS was aware that disclosure was a likely consequence of its involvement in terrorism prosecutions. Indeed, CSIS's initial experience with disclosure in the criminal justice system was a memorable, albeit unhappy one.

The SIRC report noted that CSIS was helping its employees prepare to testify in the Air India case. It raised concerns, however, 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."[60]

---

57 Ibid at 9.
58 See the case study of the *Kevork* prosecution discussed infra Part VI.
59 ibid at 18.
60 ibid at 14-15.

This report turned out to be prescient as CSIS was found to be subject to *Stinchcombe* disclosure requirements at the Malik and Bagri trial.

A second study of regional co-operation completed in 1999 also revealed that RCMP officers were concerned that CSIS officers were not disclosing to them all that they should see. These concerns were, however, denied by CSIS officers.[61] It also reported RCMP frustration that CSIS advisory letters authorized less disclosure than their initial disclosure letters. At the same time, SIRC concluded that CSIS's withholding of information to protect third party information, human sources and methods of operation "is consistent with Service policy, and is clearly stated in the terms of the Memorandum of Understanding."[62] SIRC was told that O Division had reduced its requests for disclosure letters from CSIS by 90% in large part "because the *Stinchcombe* decision had effectively turned CSIS information into what was described as a 'poison pill' when a related prosecution was initiated" [63] because of an unwillingness to disclose intelligence. It noted that some RCMP officers complained that CSIS was overprotective of its human sources, and that the police had experience with human sources and related issues of witness protection. SIRC described the disclosure issue as "what seems now to be an insoluable problem…that carried the potential to disrupt CSIS-RCMP relationships and could potentially damage the operation of both agencies."[64] The SIRC report seemed to contemplate legislation that would resolve the difficulties created by disclosure obligations, but did not outline how legislation could accomplish this task.

The 1998 and 1999 SIRC 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.

---

61 *CSIS Cooperation with the RCMP- Part 2 (SIRC Study 1998-04)* 12 Feb, 1999 at p. 5.
62 ibid at 6.
63 ibid at 7.
64 ibid at 18.

H) Post 9/11 Understandings of the Distinction Between Evidence and Intelligence

1. American Responses

The tension between the need to preserve the confidentiality of intelligence and the need to disclose evidence for trials is a universal feature of developed justice systems. As will be examined in greater detail in the seventh part of this study, many of Canada's allies have taken significant steps to facilitate the use of intelligence in criminal prosecutions. As early as 1986, one knowledgeable American commentator wrote:

> Cases dealing with classified information often cause friction between the Justice Department and the intelligence agency which has information at stake. The conflict arises because intelligence agencies are uniformly reluctant to disclose classified information, even though this information might be necessary to successfully prosecute a case. The Justice Department, on the other hand, is reluctant to proceed without advance assurances that the intelligence agency involved will declassify the necessary information. These contrary positions frequently result in an impasse and the alleged wrongdoer going free.[65]

In 1986 the conflicts between the desire to preserve the confidentiality of intelligence and to provide evidence were evident in cases in the United States, mainly in espionage cases and so- called greymail cases involving prosecutions of former officials who had access to classified information. One of the central and recurring questions for this study is whether there has been an adequate change in attitudes and practices towards intelligence and evidence in order to respond effectively and fairly to the challenges of terrorism prosecutions.

Although the United States does not have a separate domestic civilian intelligence agency such as CSIS, administrative barriers, colourfully, but not accurately, known as "the wall", were constructed to regulate the sharing of intelligence obtained under the *Foreign Intelligence Surveillance Act (FISA)* with prosecutors working on criminal prosecutions. Many of

---

65 Brian Tamanaha "A Critical Review of The Classified Information Procedures Act" (1986) 13 Am. J. Crim. L. 277 at 280-281.

these barriers were created in the wake of concerns that the Aldrich Ames espionage case might have been threatened by law enforcement uses of FISA warrants. These restrictions were then interpreted to place barriers on sharing information between FBI agents working on FISA investigations and those working on regular criminal investigations. The barriers played some role in at least one investigation of one of the 9/11 hijackers. One FBI agent working on the intelligence side rebuffed an inquiry from another FBI agent working on the law enforcement side, in part because the file contained signals intelligence. The rebuffed FBI agent working on the law enforcement side replied that "someday someone will die- and wall or not- the public will not understand why we were not more effective…Lets hope the National Security Law Unit will stand behind their decisions then, since the biggest threat to us now, bin Laden, is getting the most 'protection'." [66]

The 9/11 Commission found that the FBI intelligence agent who denied access about signals intelligence to another agent had confused matters because the suspect was already subject to a law enforcement investigation. Nevertheless, the 9/11 Commission still reached the chilling conclusion that more information sharing could have identified at least two of the hijackers and possibly disrupted the 9/11 plot.[67] It stated:

> The perception evolved into the still more exaggerated belief that the FBI could not share *any* intelligence information with criminal investigators, even if no FISA procedures had been used. Thus, relevant information from the National Security Agency and the CIA often failed to make its way to criminal investigators. Separate reviews in 1999, 2000 and 2001 concluded independently that information sharing was not occurring…Finally the NSA began putting caveats on its Bin Ladin-related reports that required prior approval before sharing their contents with criminal investigators and prosecutors. These developments further blocked the arteries of information sharing.[68]

A Joint Inquiry by Senate and House committees on intelligence also found problems with information sharing between intelligence agencies

---

66 9/11 Commission Report at 8.2.
67 9/11 Commission Report at 3.2.
68 9/11 Commission Report at 3.2.

and the FBI. It related this "breakdown of communications" to "differences in the agencies' missions, legal authorities and cultures."[69] Both the Joint Inquiry and an Inspector General's report found that the CIA failed to pass on to the FBI information about the travel to the United States of two of the 9/11 hijackers. The Inspector General commented that such information and proper operational follow-through "might have resulted in surveillance of both al Mihdhar and Al-Hazmi, surveillance in turn, would have the potential to yield information on flight training, financing and links to others who were complicit in the 9/11 attacks." [70]

The 9/11 terrorist attacks underlined the importance of sharing intelligence with law enforcement. At the same time, the post 9/11 experience with terrorism prosecutions in many countries suggests that the tensions between the desire to keep intelligence secret and the requirements for disclosure have not gone away. In some respects, they may have intensified as prosecutors argue that it is more important than ever for them to satisfy disclosure obligations in order to obtain convictions, while security intelligence agencies argue that the need to keep their ongoing operations, methods and sources confidential has increased if they are to prevent another 9/11. Although the mandates of police and intelligence agencies have become more pressing since 9/11, there is a need to rethink these mandates in light of the need to prosecute and punish terrorists.

2. British Responses

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.

---

69 Report of the Joint Inquiry into the Terrorist Attacks of 9/11 by the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence December 2002 at 77.

70 Report of the CIA Inspector General, June 2005 unclassified executive summary at xv at https://www.cia.gov/library/reports/Executive%20Summary_OIG%20Report.pdf

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**.

Our officers, working closely with members of law enforcement agencies, ensure that operations are properly co-ordinated with a view to the possible use of the resulting intelligence as evidence in court. For these reasons, as well as to ensure proper internal controls and compliance with legal obligations under the **Regulation of Investigatory Powers Act 2000 (RIPA)**, we keep detailed records of our operations, including all meetings with agents, eavesdropping, search and surveillance operations.

Judges have allowed staff to give evidence in criminal trials anonymously, including appearing behind screens. Arrangements correspond to those that have been made for undercover and specialist police officers and members of the special forces when giving evidence. The decision on these issues, however, rests with the judge in each case. Even where the judge makes an order for the screening and anonymity of Security Service witnesses, their evidence remains subject to cross-examination by the defence in the normal way.

As for relevant intelligence that is not used in evidence, the duty of prosecutors to disclose such "unused material" to the defence is set out in the **Criminal Procedure and Investigations Act 1996**. The Act does however recognise that the duty of disclosure must accommodate the need to protect sensitive information, the disclosure of which could damage important aspects of the public interest, such as national security.

Accordingly, 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)**.
>
> Claims for PII in relation to our material are made on the basis of a certificate signed by the Home Secretary. In deciding whether a claim is appropriate, the Home Secretary carries out a careful balancing exercise between the competing public interests in the due administration of justice and the protection of national security. This exercise takes account of detailed advice from prosecuting Counsel on the relevance of the material to the issues in the case.
>
> If the Home Secretary considers that the balance comes down in favour of non-disclosure, a claim for PII will be made. But the decision on a PII claim is one for the judge alone: it is the courts, not the Service or the Government, that ultimately decide what must be disclosed in a particular case. If a claim is accepted, the judge will continue to keep the decision under review throughout the proceedings.[71]

The Security Service Act, 1989 has been amended to make clear that information collected by MI5 in the proper discharge of its function can be "disclosed for the purpose of the prevention or detection of serious crime or for the purpose of any criminal proceeding".[72] A similar provision is also contained in the mandate of Britain's foreign intelligence agency.[73] There are also provisions in the *Security Service Act, 1989* that provide that one of the functions of the Security Service is to act in support of police forces and other law enforcement agencies in the prevention and detection of serious crime and that require its Director to ensure that there are arrangements for co-ordinating the activities of the Security Service with police forces, the Serious Organized Crime Agency and other law enforcement agencies. [74] Although MI5 suspended its work on serious

---

71 MI5 "Evidence and Disclosure" at http://www.mi5.gov.uk/output/Page87.html (accessed Jan 21, 2007)
72 *Security Service Act, 1989* s.2(2)
73 *Intelligence Services Act*, 1994 s.2(2).
74 *Security Service Act, 1989* ss.1(4), 2(2)(c).

crime such as drugs and arms trafficking in April, 2006 to concentrate on terrorism[75], its statutory mandate still facilitates co-ordination with the police and disclosure for the purpose of criminal proceedings.

Britain has codified common law standards of what information held by the Crown has to be disclosed to the accused so that they are considerably narrower than those that apply under *Stinchcombe* and apply only to information that could undermine the Crown's case or assist that of the accused. In addition, British terrorism prosecutions also feature requests by the Crown to the trial judge to order that intelligence not be disclosed to the accused on the basis of public interest immunity.[76] The former head of MI5 in a 2006 speech has commented that "Wherever possible we seek to collect evidence sufficient to secure prosecutions, but it is not always possible to do so: admissible evidence is not always available and the courts, rightly, look for a high standard of certainty. Often to protect public safety the police need to disrupt plots on the basis of intelligence but before evidence sufficient to bring criminal charges has been collected." [77] Dame Eliza Manningham-Buller has also recognized that intelligence can be "patchy and fragmentary and uncertain, to be interpreted and assessed. All too often it falls short of evidence to support criminal charges to bring an individual before the courts, the best solution if achievable. Moreover, as I said earlier, we need to protect fragile sources of intelligence including human sources". [78]

The divide between intelligence and evidence in Britain is dynamic. There has been an increased willingness to admit intelligence in non-criminal proceedings, where it may never be disclosed to the directly affected party and only disclosed to a security-cleared special advocate. [79] The British experience suggests that both security intelligence agencies and the courts have adjusted their procedures to respond to the challenges of terrorism prosecutions which will involve some intelligence.

---

75 MI5 "Serious Crime" at http://www.mi5.gov.uk/output/Page52.html

76 See infra part 7 for a discussion of these matters

77 Dame Eliza Manningham-Buller "The International Terrorist Threat to the United Kingdom", 2006 at http://www.mi5.gov.uk/output/Page374.html

78 Dame Eliza Manningham-Buller "The International Terrorist Threat and the Dilemmas of Countering It", 2005 at http://www.mi5.gov.uk/output/Page375.html

79 Clive Walker "Intelligence and Anti-Terrorism Legislation in the United Kingdom" (2005) 44 Crime, Law and Social Change 387.

3. Canadian Responses
i) The Anti-Terrorism Act

There have been many responses to 9/11 in Canada including an expansion of the budgets and the activities of both CSIS and CSE, the enactment of many new terrorism offences that apply to various forms of support, preparation and facilitation of terrorism, and the enactment of new regimes under the *Canada Evidence Act* to govern claims that material should not be disclosed on grounds of national security confidentiality. The *Canada Evidence Act* changes will be examined in detail in part six of the paper, but in essence they require the accused and other justice system participants to alert the Attorney General of Canada as soon as possible if they desire to use as evidence material broadly defined as sensitive and potentially injurious. The Attorney General can authorize the use of such information or challenge it before specially designated judges of the Federal Court, who will weigh the competing public interest in disclosure and non-disclosure. These judges have the ability to order disclosure, non-disclosure or partial disclosure, including the use of summaries. The trial judge is bound by non-disclosure orders, but can make any order required to protect the accused's right to a fair trial. The Attorney General can block a court order for disclosure with a certificate that can prohibit the disclosure of information relating to national security or defence or obtained from foreign entities for a fifteen-year period.

The creation of many new terrorism offences in the Criminal Code has implications for the relation between intelligence and evidence. The new offences include several offences relating to the financing of terrorism, including the provision or collection of property intending or knowing that it will be used for various forms of terrorism[80], making property or financial services available to benefit a terrorist group or intending or knowing that it will be used to facilitate terrorism,[81] using or possessing property intending or knowing that it will be used to carry out or facilitate terrorism[82], knowingly dealing or providing services in relation to terrorist property,[83] failing to disclose to the RCMP Commissioner and the CSIS Director property or transactions controlled by a terrorist group[84] and the failure of financial institutions to report on whether they

---

80 Criminal Code s.83.02
81 ibid s.83.03
82 ibid s.83.04
83 ibid s.83.08, 83.12
84 Ibid ss.83.1, 83.12

possess or control property owned by a terrorist group.[85] In addition to these financing offences, six other new terrorism offences were added to the Code. These offences apply to participating in a terrorist group for the purpose of enhancing its ability to carry out terrorism[86], facilitating a terrorist activity regardless of whether a particular terrorist activity was planned or carried out[87], committing any indictable offence for the benefit, at the direction of or in association with a terrorist group,[88] instructing a person to carry out any activity for the purpose of enhancing the ability of a terrorist group to commit terrorism[89], instructing the carrying-out of a terrorist activity[90] and knowingly harbouring or concealing someone who has carried out or is likely to carry out a terrorist activity.[91] The new Criminal Code amendments include broad definitions of a terrorist activity that includes attempts, conspiracies, counselling and threats to commit terrorist activities.

Other new crimes added to the Criminal Code by the *Anti-Terrorism Act* include threats against United Nations personnel, hate-motivated mischief relating to religious property and the placing of explosives in a public places. As with all crimes, conspiracies, attempts and counseling of these crimes could be prosecuted as separate offences before the actual crimes were committed. In addition, the *Official Secrets Act* was renamed and expanded in part to include passing on secret information to terrorist groups, asking persons to commit offences at the direction of terrorist groups or inducing persons by threat, accusation or menace to do anything that increases the capacity of a terrorist group to harm Canadian interests.

Although the precise ambit of the expansion of the criminal law is a matter of some debate, the 2001 *Anti-Terrorism Act* has criminalized a wide variety of conduct that occurs well before the actual commission of a terrorist act. The expansion of the criminal law means that what would have been, before 2001, advance intelligence that warns about threats to the security of Canada may, in some cases, now also be evidence of one of the new crimes outlined above.

The full implications of the *Anti-Terrorism Act* with respect to the relation between intelligence and evidence are only starting to become

---

85 Ibid s.83.11, 83.12
86 Ibid s.83.18
87 Ibid s.83.19
88 Ibid s.83.2
89 Ibid s.83.21
90 Ibid s.83.22
91 Ibid s.83.23

apparent. From 2001-2004, Canada relied on the use of immigration law security certificates to detain suspected terrorists. Until the Supreme Court's decision in *Charkaoui v. Canada*[92], these certificates allowed the government to both keep its own and foreign intelligence secret and to present it before the designated judge of the Federal Court in an attempt to have the certificate and the detainee's detention upheld. No criminal charges were laid under the 2001 *Anti-Terrorism* Act until 2004 and the initial prosecution has been delayed by s.38 proceedings and appeals. A second terrorism prosecution in Canada remains at a preliminary stage. Canada has had much less experience with post 9/11 terrorism prosecutions compared with Australia, the United Kingdom and the United States.

ii. The Rae Report

In 2005, the Hon. Bob Rae, in his report on the Air India bombing, stressed the need to establish a workable and reliable relation 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 secrecy and only telling others on a "need to know" basis deeply pervaded the new agency. [93]

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

---

92 2007 SCC 9
93 Hon. Bob Rae *Lessons to be Learned* (2005) at 22-23

> 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.[94]

The Rae report poses the very important question of whether traditional attitudes towards secrecy and, indeed, some of the behaviour in the Air India investigation was rooted in a Cold War paradigm in which CSIS devoted 80% of its resources to counterintelligence efforts.

Although the Rae report focuses on the changed threat environment, it also notes that better management of the relation between intelligence and evidence can have due process benefits for those accused of terrorism. Rae notes that the failure to preserve CSIS tapes on Parmar could have harmed either the state's interest in crime control or the interest of the accused in due process. The tapes could have contained incriminating evidence that could be used in criminal prosecutions, but it is also possible that they could have contained exculpatory evidence. 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. It was

---

94 ibid

only the 2005 acquittal that prevented Justice Josephson from having to craft a Charter remedy with respect to the Charter violations that he held occurred because of the destruction of the tapes and the interview notes. 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.[95]

The Rae report usefully 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 for preparation and support of terrorism.

iii. CSIS and the Conversion of Intelligence to Evidence

It is not clear whether CSIS and other security agencies have adjusted to the evidentiary implications of the expansion of the criminal law in relation to terrorism. In a speech given in March, 2002 Ward Elcock, then Director of CSIS, warned that most potential terrorists of interest to CSIS would not commit crimes and, even when they did, available evidence could not be used against them because of concerns about revealing a human source, classified technology or information obtained from foreign agencies. In his view, there was a need for an appropriate balance "between detection and forewarning and enforcement efforts". He stressed the dangers of losing "all one's intelligence assets and, therefore, any ability to monitor targets of concern down the road" for "a more minor criminal prosecution". [96] At the same time, Mr. Elcock acknowledged that the 2001 *Anti-Terrorism Act*, especially in relation to new terrorism financing offences, "will allow law enforcement agencies to succeed in dealing with terrorist activities."[97]

---

95 ibid at 16.
96 Ibid at 35, 36.
97 ibid at 36

In his 2003 John Tait Memorial Lecture, Ward Elcock elaborated on some of the differences he saw between law enforcement and security intelligence. He commented:

> Law enforcement is generally reactive; it essentially takes place after the commission of a distinct criminal offence. Police officers are results-oriented, in the sense that they seek prosecution of wrong doers. They work on a "closed" system of limits defined by the Criminal Code, other statutes and the courts. Within that framework, they often tend to operate in a highly decentralized mode. Police construct a chain of evidence that is gathered and used to support criminal convictions in trials where witnesses are legally obliged to testify. Trials are public events that receive considerable publicity.
>
> Security intelligence work is, by contrast, preventive and information-oriented. At its best, it occurs before violent events occur, in order to equip police and other authorities to deal with them. Information is gathered from people who are not compelled by law to divulge it. Intelligence officers have a much less clearly defined role, which works best in a highly centralized management structure. They are interested in the linkages and associations of people who may never commit a criminal act – people who consort with others who may be a direct threat to the interests of the state.
>
> CSIS officers make no arrests, but call upon the police of jurisdiction if apprehension is required. Their work environment is an open-ended world of nuance and shades of meaning. Information is not collected as evidence at trial but as input to the decision-making centres of government. Management control is vital in this work so that individual investigators' insights are frequently cross-checked by others, preventing personal bias from clouding the results. Finally, it is conducted in secret so that peoples' identities and reputations are protected and in order to protect the policy options of the state.

> Because of its open-ended, subtle and confidential nature, security intelligence work requires a close and thorough system of control and accountability in which political responsibility plays a large part.[98]

These comments appear to be based on a dichotomy between reactive policing and proactive and secret intelligence. As discussed above, this dichotomy reflects conventional wisdom, originating with the 1983 Pitfield report, but it makes little allowance for the challenge of terrorism prosecutions as revealed by the Air India investigation or the post-9/11 experience.

The present head of CSIS, Jim Judd, has given speeches that stress the changed threat environment faced by Canada. He has commented that "the world of 1984 when CSIS was created is a different one from the one in which we live today. At the time of its establishment, we were in the midst of the Cold War and, not surprisingly, the focus of the organization was very much on foreign espionage activities in Canada. But time moves on and national security environments evolve." In 2006, Mr. Judd described the differences between the mandate of CSIS and the police in the following terms:

> While we work closely with the RCMP and other Canadian police services, law enforcement and intelligence are two very different activities. A variety of features differentiate the two,, including:
>
> - CSIS is a civilian security intelligence agency, not a law enforcement agency – it has no powers of detention or capacity to compel cooperation and, of course, our personnel are not armed.
>
> - Our objective is to investigate threats prior to action being taken or a crime committed while police more often than not devote more time, effort and resources to investigations of crimes after they have occurred.

---

98 Ward Elcock "The John Tait Memorial Lecture" October, 2003 at http://www.csis.gc.ca/en/newsroom/speeches/speech17102003.asp?print_view=1

- As such, our principal objective is to collect intelligence and, where required, advise the Government of a potential threat. Unlike the police, we do not collect evidence per se (or collect information to evidentiary standards) to prosecute and secure convictions in court proceedings.

- CSIS has a lower threshold to undertake an investigation than do our police colleagues, ours being a "reasonable grounds to suspect" that certain activities constitute a threat to the security of Canada.

- Our mandate and authorities are set out in a single piece of legislation, enacted in 1984 and only very modestly amended five years ago in the omnibus 2001 anti-terrorism legislation.

- Our external review and oversight arrangements are different and, generally, more onerous than is the case with police services. [99]

Although clearly recognizing the changed threat environment and with some differences in tone, Mr. Judd continued to conceptualize the police role as one that mainly reacts to crime. He affirmed the CSIS role as one that does not collect evidence or "collect information to evidentiary standards."

In a speech given in April, 2008, Mr. Judd referred to "'the judicialization of intelligence'" in which intelligence was more involved in the legal process. He commented:

> One of the consequences of recent trends in anti-terrorism actions has been a growing number of criminal prosecutions that have often had at their genesis, information collected by intelligence and not law enforcement agencies.
>
> This in turn has increasingly drawn intelligence agencies in some jurisdictions into some interesting and important debates on a range of legal issues such as disclosure, evidentiary standards, and the testimony of intelligence personnel in criminal prosecutions.

---

99 Notes for Remarks at the Royal Canadian Military Institute, Toronto, Sept. 28, 2006 at http://www.csis-scrs.gc.ca/en/newsroom/speeches/speech28092006.asp

> While not startling or novel issues for the legal or police communities, these do have significant potential implications and consequences for the conduct of intelligence operations. In some instances, they have also stimulated some interesting debates over the boundary lines between law enforcement agencies and intelligence services.[100]

Mr. Judd also observed that a variety of factors including legal proceedings were driving a debate about "what is legitimately secret and what is not" and that these changes "raise the issue as to whether or not existing legislative regimes are still current".[101]

The idea that CSIS does not collect information to evidential standards has both defenders and critics. Although he is supportive of "sharing up" of information from the police to security intelligence agencies and recognizes the role of s.19 of the *CSIS Act* in authorizing "sharing down" from CSIS to the RCMP, Stanley Cohen, an experienced justice official and expert on privacy and criminal justice, has sounded several notes of caution about the use of intelligence in terrorism prosecutions. Cohen argues:

> As a general proposition, national security concerns are inconsistent with a policy of full disclosure to law enforcement, (as a threshold matter, a proper security clearance is necessary in order to obtain and hold security information). The significance of an individual criminal investigation or charge may pale in comparison to the issues at stake in a complex national security operation. Disclosure in a given case may serve to endanger operatives or reveal their identities; or tend to reveal operational techniques that should be kept secret and safeguarded.

---

100 Remarks at the Global Futures Conference, Vancouver, April 15, 2008 at http://www.csis-scrs.gc.ca/nwsrm/spchs/spch15042008-eng.asp

101 Ibid.

> Disclosures of sensitive information may potentially compromise an ongoing investigation.[102]

Cohen also expresses concerns about the privacy implications of increasing the transfer of information from security intelligence agencies to the police because "an intelligence dossier will naturally contain a range of information, including much that is unsifted or unfiltered, as well as innuendo, hearsay and speculation." Intelligence in police hands, he suggests, could lead "to dossier building and the creation of generalized suspect lists."[103] The examples of legitimate information sharing from CSIS to the RCMP cited by Cohen involve not the broad range of new terrorism offences, but other matters such as "ordinary criminal frauds, tax evasions, regulatory contraventions and so on…"[104] As will be seen, the findings of the Arar Commission support many of Cohen's concerns about the misuse of intelligence in the hands of the police. Cohen concludes that CSIS "cannot and should not become a stalking horse or proxy for law enforcement."[105]

Marlys Edwardh, an experienced criminal defence lawyer, who acted in terrorism prosecutions in the 1980's, as well as for Mr. Arar, has argued that CSIS should in some circumstances gather its intelligence to evidentiary standards. She suggests that CSIS has not learned the appropriate lessons from the Air India investigation, where it destroyed wiretaps and notes and tape recordings of crucial witness interviews. She concludes:

> CSIS policies have not changed. Two illustrations of the damage that results from this stubborn persistence will suffice. The first involves the case of Bhupinder Singh Liddar…. The [SIRC] report claimed that CSIS investigators routinely destroy screening interview notes and that

---

102 Stanley Cohen *Privacy, Crime and Terror Legal Rights and Security in a Time of Peril* (Toronto: LexisNexis, 2005) at 403. Other factors cited by Cohen include: "the fact that the disclosure of subject information may ultimately become public in an open proceeding, such as a criminal trial; the downstream implications of revealing information that may ultimately tend to reveal covert, secret or surreptitious operational practices and techniques; the need to protect sensitive sources and the requirement to adhere to agreements and undertakings with other nations in the interest of securing the nation's security and of promoting international cooperation and comity with Canada's friends and allies in the international community In addition, substantial encumbrances involving the initial acquisition of the information in question may exist that may delimit or constrain its subsequent use." Ibid at 408.

103 ibid at 404.

104 Ibid at 408. He cites a hostage taking as another example. Ibid at 406.

105 ibid at 407.

> CSIS will lie and manipulate information to achieve its ends. The second example is the case of Adil Charkaoui… Charkaoui was interviewed by CSIS and the transcripts of the interview were destroyed after CSIS summarized the interviews in accordance with CSIS policy. … The interviews took place in early 2002 – this demonstrates that the CSIS policy of evidence destruction remained in place 10 years after the SIRC 'Air India' admonition. [106]

The Supreme Court's decision in the *Charkaoui* case described above which involves destruction of CSIS notes is pending. The concerns raised by Edwardh are essentially that CSIS has not respected the due process implications of its collection of information. As the Rae report reveals, however, there are both due process and crime control consequences when CSIS does not recognize the evidentiary implications of its work in the counter-terrorism area.

iv. The Arar Commission

The Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar also examined distinctions between security intelligence and law enforcement. The Arar Commission found no fault with the decision of CSIS to hand over a series of individuals, in the immediate aftermath of 9/11, for investigation by the RCMP in the A-0 Canada investigation. Justice O'Connor stated that it was "wrong" to interpret the McDonald Commission and related reforms as "indicating that the RCMP should not be involved in any national security activities whatsoever." Although the mandates of CSIS and the RCMP are different, they also:

> …contemplate a continuum in the collection of information concerning national security threats. CSIS collects information at an earlier phase and on a broader basis than does the RCMP. It collects information and/or intelligence under section 12 of the *CSIS Act* in respect of activities that may on reasonable grounds be suspected of constituting threats to the security of Canada' and advises government of perceived threats to the security of Canada. CSIS is not a law enforcement agency, and

---

106 Marlys Edwardh "Problems of Proof in Terrorist Offences", 2006 prepared for National Criminal Law Program

> once it makes a determination that sufficient indicators of criminality are present to warrant a criminal investigation, the RCMP may become involved…
>
> In addition to conducting criminal investigations for purposes of prosecution, the RCMP has a preventive mandate under section 18 of the RCMP Act which gives it authority to conduct investigations aimed at taking steps to preserve the peace and prevent crimes.
>
> Although some have suggested that 9/11 inappropriately thrust the RCMP back into the national security business, contrary to the direction of the McDonald Commission, that is not the case. The RCMP has conducted investigations with national security implications in the years since the McDonald Commission… What has changed since 9/11 is the number and intensity of the RCMP's national security investigations and the enactment of Bill C-36 which, among other things, created new criminal offences relating to national security, as well as certain new investigative powers. In the months and years since 9/11, the RCMP has devoted a significantly larger proportion of its resources to these types of investigations, and it would seem that this higher level of activity will continue to be required for the foreseeable future.[107]

The very first recommendation made by Justice O'Connor was that "the RCMP should take active steps to ensure that it stays within its mandate as a police force to perform the duties of peace officers in preventing and prosecuting crime" and that it should respect "the distinct role of CSIS in collecting and analyzing information and intelligence relating to threats to the security of Canada."[108] Although acknowledging the need for increased co-operation and information-sharing between the RCMP and CSIS, Justice O'Connor concluded that the basic principle surrounding the separation of the security intelligence from the law enforcement function was sound.

---

107 Commission of Inquiry into the Activities of Canadian Officials in Relation to Maher Arar *Analysis and Recommendations* (Ottawa: Supply and Services, 2006) at 67-68.

108 Ibid at 312.

The Arar Commission criticized the A-O Canada RCMP investigation for failing to place restrictions or caveats on the use of information that it shared with American officials and for failing to respect restrictions on further sharing of information that it received from other agencies. It stressed the importance of both restricting the use of information that is shared, and respecting the caveats that other agencies have placed on information. Justice O'Connor observed:

> Despite this need, some RCMP officers testified that, because of the imminent threat of another terrorist attack following 9/11, it had no longer been practical or desirable at the time to adhere to polices on screening information using caveats for information shared with the United States. As some expressed it, 'caveats were down'[109]

Justice O'Connor agreed with senior RCMP officers that such an approach was not necessary even in the aftermath of 9/11. He stated:

> It is wrong to think that caveats must 'be down', to use the expression of several witnesses at the Inquiry, in order for information to be shared effectively and efficiently. Caveats should not be seen as a barrier to information sharing, especially information sharing beyond that contemplated on their face. They can easily provide a clear procedure for seeking amendments or the relaxation of restrictions on the use and further dissemination of information in appropriate cases. This procedure need not be time-consuming or complicated. With the benefit of modern communications and centralized oversight of information sharing within the RCMP, requests from recipients should be able to be addressed in an expeditious and efficient manner.[110]

Although the Arar Commission stressed the importance of caveats which restricted the subsequent use of information, it did not conceive of caveats as impenetrable barriers to the evidentiary use of intelligence. Rather, it concluded that the proper approach would be to request the originator of the information to amend the caveat to permit the use of the information in subsequent proceedings. In some cases, the originator might refuse to amend the caveats, but in other cases the caveat could be amended to

---

109 ibid at 108.
110 ibid at 339.

allow intelligence to be used as evidence, even though such uses were originally and routinely restricted.

The Arar Commission recognized some important changes in the legal and policy environment since 9/11 that have implications for the relation between evidence and intelligence. One important change was the enactment of the *Anti-Terrorism Act* that had the effect of enlarging the crime based mandate of the RCMP. In this respect, Justice O'Connor stated:

> It would be wrong, however, to conclude that respecting its institutional mandate requires the RCMP to wait until an act of terrorism has occurred before taking action. The RCMP's mandate includes preventing crime, not just investigating it after the fact. Moreover, many crimes related to terrorism are committed long before a terrorist act causes actual harm. The RCMP's mandate has always included investigating conspiracies, attempts and counselling of serious crimes. Since the enactment of the *Anti-terrorism Act*, it has also entailed investigating a broad range of acts relating to potential terrorist activities, such as the financing and counselling of terrorism, participation in terrorist groups, and related attempts, conspiracies, and threats.[111]

Although it rejected the idea that the RCMP was ever excluded from national security investigations, the Arar Commission noted the important changes of the *Anti-Terrorism Act* and how it increased the evidentiary significance of intelligence.

Another change noted by the Arar Commission was the development of "intelligence-led policing" since the early 1990's, when the RCMP recognized that its "failure to develop a sophisticated strategic as well as tactical intelligence capability" had "seriously hindered the Force's ability to accurately measure and prevent crime having an organized, serious or national security dimension in Canada, or internationally as it affects Canada."[112] It recognized that:

---

111 ibid at 313.

112 RCMP's 1991 Criminal Intelligence Program Implementation Guide as quoted Commission of Inquiry in the Actions of Canadian Officials in Relation to Maher Arar *A New Review Mechanism for the RCMP's National Security* Activities (Ottawa: Supply and Services, 2006) at 43.

> in the national security context, the very same information can be both criminal intelligence and security intelligence. It is also clear that both forms of intelligence can be gathered and analyzed in the same way. In addition while 'criminal intelligence' is collected to further the RCMP's criminal mandate, the link between the collection of intelligence and a criminal prosecution can be somewhat distant.[113]

The Commission recommended the continuation of intelligence-led policing, but with appropriate measures to ensure that it remained within the RCMP's law enforcement mandate and expertise and subject to enhanced review.

In addition, the Arar Commission documented fundamental changes in the organizational structure of national security policing in the RCMP. These changes were designed to make such policing much more centralized and better integrated with other agencies, including CSIS. These wide reaching changes included Ministerial directives issued in November, 2003, that were designed to increase centralization of the RCMP's national security investigations in order to enhance the Commissioner's operational accountability and Ministerial knowledge and accountability for high profile or controversial national security investigations. A Director General of National Security was also created in 2003 in RCMP headquarters in Ottawa, with responsibility for providing centralized approval and oversight of RCMP national security investigations. In addition, Integrated National Security Enforcement Teams (INSETS) have been created in Vancouver, Ottawa, Toronto and Montreal and include representatives of CSIS as well as representatives of other policing forces.

In its second report, the Arar Commission documented increased integration in national security activity that saw the RCMP working more closely with CSIS, a new Integrated Threat Assessment Centre, the CSE, Canadian Border Services Agency, Citizenship and Immigration Canada, the Financial Transactions Reports Analysis Centre (FINTRAC) and the Department of Foreign Affairs, among other agencies. Because of increased integration and information sharing, the Arar Commission recommended enhanced review of these agencies, including possibilities of joint and integrated review in order to mirror joint and integrated

---

113 ibid at 43.

national security activities. Although the Arar Commission did not focus on the relation between intelligence and evidence, it made findings about integration and information sharing that are consistent with an increased likelihood that intelligence collected by various domestic and foreign agencies could have an evidentiary use in national security criminal investigations or be subject to disclosure as relevant information possessed by the Crown.

v. The 2006 RCMP/CSIS MOU

A new Memorandum of Agreement signed between the Commissioner of the RCMP and the Director of CSIS in September, 2006 recognizes some of the changes outlined above. It addresses the relation between intelligence produced by CSIS and evidence that may be disclosed to the accused and used at criminal trials in a more thorough way than previous MOUs. Article 21 of the 2006 MOU provides:

> The CSIS and the RCMP recognize that information and intelligence provided by the CSIS to the RCMP may have potential value as evidence in the investigation or prosecution of a criminal offence. In these cases, the parties will be guided by the following principles:
>
> a) both parties recognize that the CSIS does not normally collect information or intelligence for evidentiary purposes;
>
> b) both parties recognize that once information or intelligence has been disclosed by the CSIS to the RCMP, it may be deemed for purposes of the prosecution process to be in the control and possession of the RCMP and the Crown and thereby subject to the laws of disclosure whether or not the information is actually used by the Crown as evidence in court proceedings;
>
> c) Sections of the *Canada Evidence Act* will be invoked as required to protect national security information and intelligence.[114]

This new MOU recognizes that information and intelligence collected by CSIS "may have potential value as evidence in the investigation or prosecution of a criminal offence." As suggested above, the many new

---

114 2006 RCMP-CSIS MOU public production no. 1374.

crimes in the 2001 *Anti-Terrorism Act* means that more CSIS information collected in counter-terrorism investigations may have evidentiary value.

The new MOU also recognizes that one of the consequences of information sharing from CSIS to the RCMP is that the information, once it is in the control of the RCMP and the Crown, may have to be disclosed to the accused. This reflects the importance of the *Stinchcombe* disclosure obligations. Finally, the new MOU recognizes the ability of the Attorney General of Canada to use the enhanced provisions of the *Canada Evidence Act* to protect national security and intelligence from disclosure. As will be discussed below, these powers include not only the ability to make *ex parte* submissions to the Federal Court about the dangers of disclosure, but also to counter court-ordered disclosure with an Attorney General's certificate that will prohibit all disclosure of information relating to national defence or national security or obtained from foreign sources for a fifteen year period. The MOU indicates a growing awareness of the close connection between intelligence and terrorism in the post 9/11 era. At the same time, however, invocation of the enhanced provisions in s.38 of the CEA is not a panacea. As will be seen in subsequent sections, they fragment and prolong criminal trials.

I) Summary

Although the RCMP and CSIS retain and should respect their different mandates, they operate in a dynamic legal and policy environment. The crime prevention and evidence collection mandate of the RCMP has been increased with the enactment of the 2001 ATA. This law contains many new terrorism offences that will be complete long before any act of terrorism. 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. 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 dichotomies between reactive policing and proactive intelligence; between decentralized policing and centralized intelligence and between secret intelligence and public evidence. All of these dichotomies are based on

the prevailing attitude at the time CSIS was created in 1984 during the Cold War, even though a close reading of the *CSIS Act* and *Security Offences Act* reveals 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 in 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 with the demands of the collection of evidence. In this respect, it is noteworthy that MI5 accepts the need to collect some evidence (albeit not electronic surveillance which is still generally inadmissible in British courts) to an evidentiary standard. Requests may have to be made to foreign agencies to 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 the *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

The following four principles are broadly consistent with the seven principles identified by Bruce MacFarlane in his companion study on structural aspects of the criminal trial. In other words, the principles articulated here encompass the values of respect for the rule of the law