When Secret Intelligence Becomes Evidence: Some Implications of Khadr and Charkaoui II

Kent Roach

Follow this and additional works at: http://digitalcommons.osgoode.yorku.ca/sclr

This work is licensed under a Creative Commons Attribution-Noncommercial-No Derivative Works 4.0 License.

Citation Information
http://digitalcommons.osgoode.yorku.ca/sclr/vol47/iss1/6

This Article is brought to you for free and open access by the Journals at Osgoode Digital Commons. It has been accepted for inclusion in The Supreme Court Law Review: Osgoode’s Annual Constitutional Cases Conference by an authorized editor of Osgoode Digital Commons.
When Secret Intelligence Becomes Evidence: Some Implications of Khadr and Charkaoui II

Kent Roach*

I. INTRODUCTION

Jim Judd, the outgoing head of the Canadian Security Intelligence Service (“CSIS”), has listed “the judicialization of intelligence” as one of the major changes affecting intelligence agencies. The judicialization of intelligence is a process in which intelligence agencies have to confront, often for the first time, “a range of legal issues such as disclosure, evidentiary standards, and the testimony of intelligence personnel in criminal prosecutions.” Mr. Judd made these remarks on April 15, 2008. In what is surely an admirable quality in the head of an intelligence agency, he accurately predicted the future.

A month after Judd’s speech, the Supreme Court of Canada released its decision in the Omar Khadr case. Subject to subsequent national security confidentiality proceedings under section 38 of the Canada

* Professor of Law and Prichard-Wilson Chair in Law and Public Policy, University of Toronto. I thank Anil Kapoor for helpful comments on an earlier draft.


He added that such issues, 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.

He also noted a trend to increased transparency adding that “It is quite likely, I think, that the more information that goes into the public domain the greater will be the pressure to make even more known, in the process calling into question the legitimacy of secrecy.” For a somewhat more optimistic take on the role of courts and intelligence agencies, see Fred Manget, “Intelligence and the Rise of Judicial Intervention” in Loch Johnson, ed., Handbook of Intelligence Studies (Oxford: Routledge, 2007). Manget, a former Deputy General Counsel of the CIA, concludes (id., at 340):
The involvement of the federal judiciary is limited but salutary in its effect on executive branch actions. Nothing concentrates the mind and dampens excess so wonderfully as the imminent prospect of explaining one’s action to a federal judge … Federal judges are the essential third part of the oversight system in the United States, matching requirements of the law to intelligence activities and watching the watchers.
Evidence Act, CSIS would have to disclose the fruits of its interviews with Omar Khadr at Guantanamo Bay, Cuba as well as the information that CSIS subsequently shared with American officials as a result of those interviews. The very next month, the Supreme Court released Charkaoui v. Canada (Citizenship and Immigration), holding that CSIS breached its duties under section 12 of the Canadian Security Intelligence Service Act when it destroyed the operational notes of interviews it conducted with security certificate detainee Adil Charkaoui. Taken together, these two decisions highlighted that CSIS has constitutional and statutory duties to retain and disclose secret intelligence.

A third decision, R. v. McNeil, decided by the Supreme Court in early 2009, also fits into the trend of CSIS being subject to increased disclosure obligations. Although this decision affirmed that not all government agencies will be subject to R. v. Stinchcombe disclosure obligations, it also held that an “investigating state authority” may be subject to Stinchcombe obligations to disclose the fruits of the investigation. This raises serious questions of whether CSIS will be held to be an investigating state authority when it investigates threats to national security and in particular terrorism. In any event, McNeil narrows the gap between CSIS being subject to Stinchcombe disclosure obligations and being subject to R. v. O’Connor third party production obligations by suggesting that the Crown has an obligation to bridge any gap by inquiring about known and relevant information held by another agency. Crowns will have to inquire whether CSIS has relevant information in most terrorism prosecutions. The gap was also narrowed by the Court’s ruling in McNeil that truly relevant information held by third parties will generally have to be disclosed absent successful claims of privilege.

Although Khadr and Charkaoui II were made outside of the criminal context, they, when combined with McNeil, have implications for the retention and disclosure of intelligence in terrorism prosecutions. For

---

10 McNeil, supra, note 6, at paras. 47-51.
11 Id., at para. 41.
example, CSIS’s destruction of intelligence in the Air India trial violated the accused’s rights under section 7 of the *Canadian Charter of Rights and Freedoms* and the recently completed Khawaja terrorism prosecution featured extensive litigation over whether CSIS intelligence had to be disclosed to the accused. The Court in *Charkaoui II* significantly qualifies the traditional idea that CSIS is a security intelligence agency that should not be concerned with the collection of evidence or the evidentiary implications of its actions. Although CSIS was never intended to be and is not a police force, “the activities of the RCMP and those of CSIS have in some respects been converging as they, and the country, have become increasingly concerned about domestic and international terrorism.” *Charkaoui II* is a wake-up call that recognizes the need to interpret the CSIS Act enacted in 1984 in light of changed circumstances, as Canada has emerged from a Cold War era, in which intelligence could always be kept secret, into a post-Air India and September 11 era, in which intelligence investigations of suspected terrorists can quickly become matters in which arrests and subsequent legal proceedings are required.

The obligations to retain and possibly to disclose intelligence imposed on CSIS are broader in *Charkaoui II* than they are in *Khadr*. The Court in *Charkaoui II* interprets section 12 of the CSIS Act, which applies to the collection, retention and analysis of all CSIS intelligence relating to security threats. The Court supports its interpretation of section 12 by reference to section 7 of the Charter, which it affirms applies to security certificate proceedings under immigration law because “the consequences of security certificates are often more severe than those of many criminal charges.” At the same time, however, the decision remains a general interpretation of section 12 of the CSIS Act as it applies to all of CSIS’s activities.

The Court’s decision in *Khadr* is narrower than *Charkaoui*. The ambit of CSIS’s disclosure obligations in *Khadr* is framed not by section

---

16 *Id.*, at para. 54.
12 of the CSIS Act or by Stinchcombe, but by the precise scope of the violation of international law that required extra-territorial application of the Charter. In this sense, the Court’s decision follows the restrictive approach to the extra-territorial application of the Charter in R. v. Hape. The Supreme Court’s decision in Khadr is also narrower than the Federal Court of Appeal’s appeal decision in the same case which applied broad Stinchcombe disclosure obligations. It will be suggested in this essay that the restrictive nature of the disclosure obligation in Khadr is regrettable because the Court could have defined the disclosure obligation more broadly while still allowing the government an opportunity to justify exceptions to it on the grounds that the information was not relevant to Omar Khadr’s defence or because of particular harms that disclosure would cause to national security, national defence or international relations.

The Supreme Court’s decisions in Khadr and Charkaoui II have the potential to subject CSIS’s secret intelligence to the rule of law, external verification and adversarial challenge in legal proceedings. The disclosure of CSIS intelligence provides a vehicle for the objects of intelligence (or security-cleared special advocates acting on their behalf) to challenge the accuracy and reliability of intelligence that would normally not see the light of day. The findings of the Arar Commission that the RCMP passed on inaccurate and unfair intelligence labelling Maher Arar and his wife as Islamic extremists associated with Al Qaeda underline the damage that inaccurate intelligence can cause to individuals in a world where intelligence can be transferred within and between governments with the click of a send button. The disclosure of intelligence can serve as another instrument of accountability for CSIS.

Although the Court’s ruling about the importance of retention of intelligence in Charkaoui could have positive benefits in terms of increased adjudicative fairness and increased accountability for CSIS, it could also lead to increased retention of intelligence files and as such have negative impacts on privacy. If CSIS adjusts its practices to respond to the new imperatives of retention and disclosure of intelligence, it will be important that its review bodies remain vigilant that CSIS only collect

---

17 Supra, note 7.
19 Supra, note 7.
20 Commission of Inquiry into the Activities of Canadian Officials in Relation to Maher Arar, Analysis and Recommendations (Ottawa: Supply and Services, 2006), at 24-25.
intelligence to the extent that it is strictly necessary to fulfil its statutory mandate. It will also be important that review bodies have the ability to follow intelligence that CSIS may share with other agencies. Unfortunately, the Canadian government has still not responded to the recommendations made by the Arar Commission that were designed to strengthen the review of national security activities with special attention to increased information sharing and integration between the RCMP, CSIS and other agencies with national security responsibilities.\(^2\)

The Court’s decisions in \textit{Khadr} and \textit{Charkaoui II} should mean that more intelligence including “raw” intelligence in the form of original and operational notes and recordings should be retained by CSIS, but it does not necessarily mean that such intelligence will be disclosed in legal proceedings. In both cases, the Court stressed that disclosure would not be automatic and that the government would have an opportunity to justify non-disclosure on grounds related to the harms that disclosure would cause to national security. In \textit{Khadr}, the government could seek non-disclosure orders under section 38 of the \textit{Canada Evidence Act} and the Federal Court judge would balance and reconcile the competing interests in disclosure and non-disclosure. In \textit{Charkaoui}, the Court accepted that the judge would filter and summarize the intelligence that could be disclosed to the detainee on standards under the \textit{Immigration and Refugee Protection Act}\(^2\) that are even more protective of state interests in secrecy than those under section 38 of the \textit{Canada Evidence Act} because they prohibit the disclosure to the detainee and the public of all information that, if disclosed, would harm national security or persons. The Court’s caution in both cases about the actual disclosure of intelligence to the directly affected person is consistent with the Court’s caution in other cases about the dangers of disclosing intelligence especially given Canada’s position as a net importer of intelligence.\(^3\) Courts will have to reject the overclaiming of secrecy if the promise of disclosure of intelligence offered in \textit{Khadr} and \textit{Charkaoui} is to be made real.

\(^{2}\) Commission of Inquiry into the Activities of Canadian Officials in Relation to Maher Arar, \textit{A New Review Mechanism for the RCMP’s National Security Activities} (Ottawa: Supply and Services, 2006).

\(^{3}\) S.C. 2001, c. 27.

In order to appreciate the potential magnitude of the change that could be caused by Khadr and in particular Charkaoui, a little history is necessary. The second part of this paper will provide an overview of the evolution of Canadian approaches to secrecy and the use of intelligence as evidence. The changes in these areas have been rapid and profound. Until 1982, Ministers were able to assert an essentially unreviewable discretion to prevent the disclosure of intelligence on grounds of harms to national security. Although the Federal Court was given jurisdiction to order the disclosure of intelligence in 1982, it exercised this jurisdiction very cautiously in the last days of the Cold War, sometimes not even examining secret intelligence before ordering that it not be disclosed.

In the post-September 11 environment, there are signs of change, including an increased skepticism to claims that the non-disclosure of intelligence is justified by concerns about the mosaic effect in which the disclosure of even innocuous intelligence can assist the enemy. There is also a recognition that while Canada remains a net importer of intelligence, it still can and should request foreign agencies to consent to the disclosure of intelligence. Other factors leading to increased attempts to obtain the disclosure of intelligence are increased use of security certificates under the immigration law as a form of anti-terrorism law and the broad new terrorism offences found in the Anti-Terrorism Act which can make much intelligence relevant to the prosecution process.

The third part of this paper will assess the Supreme Court’s decision in Khadr v. Canada with an emphasis on its holding about the disclosure of intelligence collected and disseminated by CSIS more than on its holding about the extra-territorial application of the Charter. That said, it will be seen that the topics are linked because the Court restricted the ambit of CSIS material subject to disclosure on the basis of its understanding of the scope of the conduct that violated international law and required an extra-territorial application of the Charter and a finding of a Charter violation. The disclosure obligations in Khadr were shaped by the limited scope of the Charter violation. They were not shaped by the concern in Stinchcombe that the accused should have access to all relevant and non-privileged material in order to assist in his or her defence. A broader definition of what had to be disclosed in Khadr would not have been determinative because the Court contemplated that

---

the government would be able to claim national security confidentiality and other privileges before any information was actually disclosed to Omar Khadr. Subsequent decisions about the ambit of actual disclosure in this case will also be briefly examined.

The fourth part of the paper will focus on the Court’s decision in *Charkaoui II* with respect to the proper interpretation of section 12 of the CSIS Act as it relates to the retention of intelligence collected about individuals and groups. As will be seen, the Court’s interpretation of this provision was influenced by its interpretation of section 7 of the Charter and its preference that the Ministers who issue security certificates and the judges who review security certificates have all of the relevant information, including raw intelligence, available to them. This part of the decision was based on a healthy skepticism about relying simply on CSIS’s analysis and conclusions without verification against the raw intelligence. Indeed, the Court’s decision that the original intelligence should be retained was justified in large part on the basis that retention would allow CSIS, Ministers and eventually judges to verify the correctness of CSIS’s analysis and conclusions about the raw intelligence against the original data. The Court took notice of inaccurate intelligence in both the Maher Arar and Bhupinder Liddar cases and made five references to the need for verification of analysis against original intelligence in a relatively short 78-paragraph judgment. The possibility

---

26 Mr. Liddar complained to the Security Intelligence Review Committee after being denied a security clearance necessary for a diplomatic posting.

After reviewing the complaint, SIRC found there was no reasonable basis for that recommendation, and that it was inaccurate and misleading for several reasons. First, SIRC concluded that the denial brief contained an unfair and prejudicially inaccurate account of the information that the Service had in its possession when it began the security clearance investigation. Next, SIRC concluded that the brief was based on a field investigation conducted by an inexperienced CSIS investigator, who arrived at unfounded conclusions. SIRC found that there was no reliable evidence to support a conclusion that the complainant might engage in activities that would constitute a threat to the security of Canada, or that the complainant might disclose classified information in an unauthorized way.

SIRC Annual Report 2005-2006, at 22-23, available online: <http://www.sirc-sics.gc.ca/anrran/2005-2006/index-eng.html> [hereinafter “SIRC Annual Report”]. SIRC noted that the CSIS investigator was not able to provide it with the answer that Mr. Liddar gave at his security clearance interview and that this reflected “a long-running concern of the Review committee with respect to the CSIS practice of destroying the notes that the investigators take of security screening investigations”. As quoted in *Charkaoui II, supra*, note 4, at para. 40. SIRC recommended that “CSIS institute procedures to ensure that accurate notes are taken, or that a recording is made, of security screening interviews. These should be kept for five years after an interview, or for even longer periods should an interviewee challenge the outcome of a security screening investigation.”

SIRC Annual Report, id., at 22.

27 *Charkaoui II*, id., at paras 39, 56, 62, 63, 73.
of inaccurate intelligence conclusions and analysis was definitely on the Court’s mind when it concluded that CSIS must no longer destroy the raw intelligence it collects about individuals.

Although the Court stressed the importance of retention and disclosure of intelligence for adjudicative fairness, its decision will not mean that security certificate detainees will have direct access to the intelligence if its disclosure would harm national security or endanger other persons. As in Khadr, intelligence would be filtered and summarized in order to protect national security interests before being disclosed to the detainee. In addition, unfiltered intelligence could be disclosed to the security-cleared special advocates who have been appointed in the wake of the Court’s decision in Charkaoui I holding that the complete lack of adversarial challenge to the intelligence used to support detention and possible deportation under a security certificate violated section 7 of the Charter.

The fifth part of this paper will examine some possible harms and benefits of the judicialization of intelligence promoted by Khadr and Charkaoui II. I will argue that the judicialization of intelligence is generally a positive development that is part of an ongoing process of subjecting CSIS to the rule of law and subjecting its conclusions and analysis to validation and adversarial challenges that can expose errors, exaggerations and speculation in analytical conclusions. The retention of raw intelligence can increase CSIS’s internal and external accountability by creating the conditions under which its conclusions can be checked against its raw data. The retention of raw intelligence can also increase the adjudicative fairness of security certificate proceedings, terrorism prosecutions and challenges to the denial of security clearances by facilitating fuller adversarial challenge to the evidence provided by CSIS and others in such cases. Increased retention of raw intelligence can also make it easier for CSIS to work with law enforcement agencies. Although subsequent terrorism prosecutions will still involve section 38 proceedings to determine whether intelligence must be disclosed to the accused, retention of intelligence can avoid findings that section 7 of the Charter has been violated by the destruction of relevant intelligence. That said, the immediate effect of Charkaoui II will be to inspire requests for remedies for the destruction of raw intelligence pursuant to long-standing but now invalid CSIS policies.

The judicialization of intelligence is not without its dangers. It could lend a perhaps unwarranted legitimacy to the use of intelligence as evidence in the security certificate process. Intelligence, even intelligence
that is verified against the raw data, may still be speculative. Moreover, intelligence may still be erroneous if the raw data, data that may have been collected by a foreign agency, is itself erroneous or is shaped by confirmation bias or what a number of inquiries into miscarriages of justice have coined as “tunnel vision”. As will be seen, some leading intelligence practitioners and scholars are starting to recognize that intelligence collection and analysis may be distorted by a variety of cognitive biases including confirmation bias. Although retention and disclosure of raw intelligence provides some protection against tunnel vision, it does not guarantee that the raw intelligence itself will not be shaped and limited by the cognitive biases and limitations of the investigators.

In addition, the promise of disclosure offered by Khadr and Charkaoui II might not be fulfilled if national security confidentiality can successfully be overclaimed by the government to prevent full disclosure or if special advocates who receive intelligence are unable to engage in consultations with detainees and others that may be necessary to provide effective adversarial challenge to the intelligence.

The Court in Charkaoui II only partially recognizes the potential effects of increased retention of intelligence on privacy. The Court concludes that the risks to privacy by retention of raw intelligence are justified when CSIS “targets a particular individual or group” as opposed to conducting investigations “of a general nature”. This distinction recognizes the demands of adjudicative fairness, but the Court may not have fully appreciated how many CSIS investigations target individuals or groups. The most recent public information about CSIS targeting practices suggests that over 90 per cent of the targets of CSIS

---


29 Richard J. Heuer, Jr., Psychology of Intelligence Analysis (New York: Nova Publishers, 2006), at 28, 41, 59, 175 [hereinafter “Heuer”]. The author of this book worked for the CIA from 1951 to 1979, retiring as the head of the methodology unit for the Director of Intelligence. Id., at 7. The book devotes five chapters to various forms of cognitive biases that can affect the analysis of intelligence including confirmation bias. It concludes that “significant biases in the evaluation of intelligence estimates are attributable to the nature of human mental processes, and not just to self-interest and lack of objectivity, and that they are, therefore, exceedingly difficult to overcome.” Id., at 175.


31 Charkaoui II, supra, note 4, at para. 43.
investigations are individuals or groups as opposed to issues or events.\textsuperscript{32} If this continues to be the case, and there is no reason why CSIS should not focus on individuals and groups as opposed to issues and events, it will be very important that CSIS observes the limits of its statutory mandate when engaging in targeted investigations and that its review bodies remain vigilant to these limits.

II. THE CHANGING RELATIONSHIP BETWEEN SECRET INTELLIGENCE AND PUBLIC EVIDENCE FROM THE COLD WAR TO MASS TERRORISM

Intelligence agencies have not traditionally had to worry about the disclosure of intelligence in legal proceedings. Intelligence was collected to be distributed within government to those with appropriate security clearances. Espionage and other prosecutions that might involve the disclosure of intelligence were possible but exceedingly rare. Until 1982, those who collected intelligence in Canada could be secure in the knowledge that the government could assert absolute secrecy claims to protect intelligence from disclosure.

1. The Cold War and Absolute Secrecy

In 1982, the Quebec Human Rights Commission attempted to challenge the invocation of national security privilege when investigating the reasons why a switchboard operator and a waitress had been dismissed for security reasons from their jobs working at the 1976 Montreal Olympics. The Supreme Court of Canada unanimously dismissed the Commission’s challenge to the absolute national security provisions then in force under section 41(2) of the Federal Court Act.\textsuperscript{33} The provision precluded judges from even examining material once a Minister of the Crown certified that the disclosure of the document would be injurious to international relations, national defence or security. The Commission’s arguments at the time were not without force. Its enabling statute clearly gave the Commission all the powers of a superior court and the common law in Britain had already moved away from an absolute understanding of national security confidentiality.\textsuperscript{34}

\textsuperscript{32} SIRC Annual Report, supra, note 26, Table 3, at 38.
\textsuperscript{33} R.S.C. 1970, c. 10 (2nd Supp.).
\textsuperscript{34} Conway v. Rimmer, [1968] A.C. 910 (H.L.).
Justice Chouinard for a unanimous Court upheld the absolute privilege on the basis that “saying that Parliament and the legislatures cannot make the privilege absolute amounts to a denial of parliamentary supremacy.”\(^{35}\) He also quickly dismissed a Canadian Bill of Rights challenge on the basis that while the absolute privilege “does of course create in favour of the Crown, the guardian of the nation’s higher interests, a regime which differs that applicable to individuals”,\(^{36}\) the result did not infringe the right of individuals to equality before the law. It is difficult to imagine a decision that was more the antithesis of the rule of law and accountability than this decision by the Supreme Court. Yet this decision was made only 27 years ago and in the year that the Canadian Charter of Rights and Freedoms was proclaimed in force.

Although judges after 1982 were given the power to review secret information to determine whether it should be disclosed, old habits died hard. In 1984, the Federal Court of Appeal unanimously upheld the non-disclosure of secret information that former RCMP officers claimed could provide them with a defence with respect to charges that they had stolen the Parti Québécois’ membership list. The Court of Appeal approved of the non-disclosure of information that it had not even examined, with Le Dain J.A. expressing doubts about the competence of the Court to determine the sufficiency and adequacy of restrictions on disclosure and Marceau J.A. stating that “to accept that national security and international relations be injured, even to only the slightest extent, in order that such a remote risk of extreme incredulity on the part of 12 members of a jury be avoided, would appear to me, I say it with respect, totally unreasonable.”\(^{37}\)

A similar categorical if not cavalier approach to the preference of the state’s interests in protecting secrets over the accused’s interests was demonstrated the next year when those accused of terrorism were denied access to CSIS surveillance material on them despite the possibility that the surveillance could possibly have revealed exculpatory material such as the whereabouts of the Toronto-based accused who were accused of an attempted assassination of a Turkish official in Ottawa. Again, the Federal Court chose not to exercise its new powers to look at the secret documents. Justice Addy of the Federal Court refused to allow the Director of CSIS to be cross-examined on his affidavit and held that


\(^{36}\) Id., at 230.

the mere fact that Parliament has chosen to allow this court to consider
an objection to disclosure on grounds of national security, national
defence or international relations when the subject matter was
previously within the exclusive realm of the executive arm of
government, is not any indication that it is any way less important than
before the statutory enactment.\textsuperscript{38}

In other cases, Addy J. expressed concerns that pursuant to the so-called
mosaic effect, the disclosure of even innocuous information could harm
national security and that great danger could be caused by the disclosure
of any of CSIS’s methods, targets or members.\textsuperscript{39} The accused’s attempts
to obtain disclosure was dismissed as “a fishing expedition” with the
judge opining that the accused’s attempt to use intelligence material to
impugn the credibility of a witness was “merely a side issue” in a
criminal trial.\textsuperscript{40} The trial judge in this case eventually held that a fair trial
was still possible in light of non-disclosure, but expressed considerable
unease with the fact that only specially designated judges of the Federal
Court could examine the information and no judge had in fact examined
the secret information in this case.\textsuperscript{41}

2. Emerging Rights to Disclosure

There were some decisions in the 1980s that demonstrated the
possibility that intelligence might have to be disclosed in order to respect
the Charter rights of the accused to disclosure and to make full answer
and defence. For example, Watt J. held that disclosure was necessary in a
case involving Talwinder Singh Parmar, widely believed to have been
the mastermind of the 1985 Air India bombings that killed 331 people.
He reasoned that even if the accused’s disclosure requests were the
proverbial “fishing expedition”, they were now one that was conducted in
“constitutionally protected waters”.\textsuperscript{42} In the wake of his ruling that a
wiretap warrant could not be supported by material involving a
confidential source that was not disclosed to the accused, the prosecution
against Parmar and others alleging a conspiracy to commit acts of


\textsuperscript{40} Re Kevork, supra, note 38, at 434-35.


terrorism in India was abandoned. Around the same time in the late 1980s, the Federal Court of Appeal ordered that an affidavit used to obtain a wiretap under the CSIS Act should be disclosed to the accused. Once inaccuracies in the affidavit were revealed as a result of its disclosure, the then Director of CSIS Ted Finn resigned and another conspiracy to commit terrorism prosecution was abandoned.\(^43\) CSIS’s initial experience with court ordered disclosure was not a happy one.

3. The Origins of the CSIS Act

There was a tendency at the time that CSIS was created in 1984 to stress the differences between the collection of intelligence as opposed to evidence. This emphasis was related to the desire not to give the new civilian intelligence agency law enforcement powers. Although the McDonald Commission recognized that a security intelligence agency might have to work with law enforcement with respect to matters such as espionage, terrorism and subversion, it stressed “fundamental differences between most police work and security intelligence responsibilities … The main product of security intelligence work takes the form of advice to both government and regular police forces” consisting of “raw information” and “analysis”.\(^44\) The implicit assumption, so entrenched that it was not mentioned, was that intelligence would be secret.

Other parts of the McDonald Commission also reflected Cold War assumptions. For example, it stated that “by far the most important” reason behind the “need to know” principle “is the need to minimize the damage of an unknown penetration by an enemy agent”.\(^45\) The McDonald Commission recognized that section 41 of the Federal Court Act allowed Ministers of the Crown to withhold information from the courts on the grounds that disclosure of the information would harm national security.\(^46\)

Much of the debate that followed the McDonald Commission’s report and led to the enactment of the CSIS Act in 1984 stressed differences between police and security intelligence work. One of the prime differences was that the work of the police would eventually become public and subject to challenge in court while the work of

\(^{45}\) Id., at 745.
\(^{46}\) Id., at 661.
security intelligence agencies would remain secret. The most frequently quoted passage in this regard was the following statement taken from a Special Senate Committee chaired by Michael Pitfield that reported in 1983. The Pitfield Committee stated:

Law enforcement is essentially reactive. While there is an element of information-gathering and prevention in law enforcement, on the whole it takes place after the commission of a distinct criminal offence. The protection of security relies less on reaction to events; it seeks advance warning of security threats, and is not necessarily concerned with breaches of the law. Considerable publicity accompanies and is an essential part of the enforcement of the law. Security intelligence work requires secrecy. Law enforcement is “result-oriented”, emphasizing apprehension and adjudication, and the players in the system — police, prosecutors, defence counsel, and the judiciary — operate with a high degree of autonomy. Security intelligence is, in contrast, “information-oriented”. Participants have a much less clearly defined role, and direction and control within a hierarchical structure are vital. Finally, law enforcement is a virtually “closed” system with finite limits — commission, detection, apprehension, adjudication. Security intelligence operations are much more open-ended. The emphasis is on investigation, analysis, and the formulation of intelligence.47

In this passage, a stark contrast was drawn between the reactive work of the police and the proactive work of security intelligence agencies. This discounted the crime prevention role of the police as well as their responsibility to enforce the law with respect to inchoate offences such as conspiracies and attempts. The Pitfield Committee ignored the overlapping jurisdiction of the police and security intelligence agencies with respect to terrorist plots that would be both threats to the security of Canada and crimes. The Committee also assumed that all of the work of the police would be made public and discounted the ability of the legal system to protect some intelligence from disclosure through devices such as public interest immunity and evidentiary privileges. At the same time, it also assumed that all security intelligence required secrecy. This assumption made some sense with respect to the counter-intelligence work of a security intelligence agency in the Cold War, but much less sense with respect to terrorist threats.

The CSIS Act itself also placed considerable emphasis on maintaining the secrecy of intelligence. Although it gave those denied security clearances the right to complain to the Security Intelligence Review Committee (“SIRC”), complainants do not have a right to be present during SIRC hearings48 and SIRC is bound by all the security requirements and secrecy oaths that apply to CSIS employees.49 The secrecy of spying is also acknowledged in section 18 of the CSIS Act. The section makes it an offence, subject to some exceptions, to disclose information obtained under the Act that could reveal the identity of confidential sources of information or employees engaged in covert operational activities. That said, section 19 of the CSIS Act contemplated from the start that intelligence could be relevant to police investigations and prosecutions and might have to be disclosed to that end. Nevertheless, section 19 provides CSIS with a discretion not to disclose such intelligence. To the extent that intelligence is used for preventive purposes, there was a reasonable expectation that it could remain secret forever and not have to be disclosed to directly affected people or the public in legal proceedings.

4. Changing Approaches to Secrecy

As discussed above, the emphasis on fair trial rights and disclosure under the Canadian Charter of Rights and Freedoms exerted some pressure in the late 1980s towards the disclosure of intelligence. This pressure came in prosecutions launched in the wake of the 1985 bombings of Air India, events that resulted in the deaths of 331 people in what was, before September 11, 2001, the most deadly act of aviation terrorism in history. Even after September 11, however, there were some who clung to Cold War era ideas that secrecy was an absolute value and that CSIS’s security intelligence mandate meant that it did not collect evidence or have to worry about the evidentiary effects of its practices including its frequent destruction of raw intelligence. In his 2003 John Tait memorial lecture, then CSIS Director Ward Elcock returned to many of the ideas expressed 20 years earlier by the Pitfield Committee when he stated:

Law enforcement is generally reactive; it essentially takes place after the commission of a distinct criminal offence. Police officers are

48 CSIS Act, s. 48(2).
49 Id., s. 37.
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.

The Special Senate Committee remarked in 1983 that security work requires a different background than police work ... one that is embodied in a new type of recruit with a different outlook and education, emphasizing analytical and assessment skills. Events that resulted in the creation of the CSIS Act and the Service also led the Committee to conclude that a civilian organization would best assure the necessary political control.50

In this passage, the then Director of CSIS reiterated the stark dichotomy between reactive policing and proactive and secret intelligence that had been articulated 20 years earlier in the Pitfield Report. There was little, if

any, recognition that CSIS would have to change in response to its overlapping jurisdiction with the RCMP with respect to the activities of suspected terrorists that could also be crimes, including the many new crimes of facilitating and financing terrorism and participating in a terrorist organization that Canada created shortly after September 11.\footnote{Criminal Code, R.S.C. 1985, c. C-46, Part II.1.}

The above approach with its emphasis on secrecy and the idea that CSIS does not collect evidence can be contrasted with that taken by Bob Rae in his 2005 review of the Air India bombing. Rae observed that at the time of the creation of CSIS in 1984 “counter-intelligence (as opposed to counter-terrorism) took up 80 per cent 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.” Rae commented on the dangers of excessive secrecy and a silo-based approach in which security intelligence and the police were reluctant to share information. Reflecting on CSIS’s destruction of wiretaps and original notes that were held by Josephson J. in the Air India trial to have violated the rights of the accused under section 7 of the Charter, Rae commented that:

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.\footnote{Bob Rae, Lessons to be Learned (Ottawa: Public Safety, 2005), at 22-23.}

Rae’s approach recognized that CSIS’s original attitudes towards secrecy were rooted in the Cold War and that a changed threat and legal environment meant that in some cases intelligence would have to be disclosed in legal proceedings or even used as evidence.

The 1983 Pitfield Report was considered by the Supreme Court in Charkaoui II. The Supreme Court accurately noted that the Pitfield Report “stressed the distinction between the policing function and the role of an intelligence agency. Law enforcement agencies generally react to the commission of criminal offences, whereas those responsible for
prevention and for the protection of security must try to anticipate threatening events. Significantly, however, the Court suggested that the stark dichotomy between security intelligence and policing made in the Pitfield Report and accepted by Noel J. in his ruling in Charkaoui II that CSIS was not subject to any disclosure duty because it was not a police force was no longer quite accurate. Justices LeBel and Fish stated:

CSIS is not a police force. This is clear from the legislative history set out above. In reality, however, it must be acknowledged that the activities of the RCMP and those of CSIS have in some respects been converging as they, and the country, have become increasingly concerned about domestic and international terrorism. The division of work between CSIS and the RCMP in the investigation of terrorist activities is tending to become less clear...

This was an important recognition by the Supreme Court that both the threat and legal environment had significantly changed since 1983. In short, Canada had moved from the Cold War to an age in which security intelligence and the police must work together to prevent lethal acts of mass terrorism. In such an environment, CSIS can no longer afford to destroy intelligence in the name of secrecy.

There are signs of increased recognition that a secrecy culture that may have been necessary to avoid penetration by the KGB during the Cold War may not be appropriate today. The Federal Court has abandoned its prior practices of not examining secret information. In a number of decisions it has expressed skepticism that reliance on the Cold War concept of the mosaic effect — namely, that the disclosure of innocuous information may still benefit the enemy — can in itself justify non-disclosure on national security grounds. The Federal Court has also recognized that while the third party rule still appropriately prevents the disclosure of information provided in confidence to Canada by foreign agencies that Canada should request the foreign agencies to consider providing their permission for the subsequent disclosure of information. The Court has also recognized that the third party rule should not be used

53 Charkaoui II, supra, note 4, at para. 23.
to prevent the disclosure of intelligence that is already in the public domain. Justice O’Connor has warned about the dangers of overclaiming secrecy because of its adverse effects on the fairness and transparency of proceedings, as well the credibility of the government’s attempt to protect secrets that must be protected.

In his 2008 John Tait Lecture, John Sims, the deputy Attorney General of Canada, reflected on the 1983 Pitfield dichotomy between the secret work of intelligence agencies and the public work of the police when he stated that

the primary mandate for the new security intelligence agency was intended to be the provision of confidential “intelligence” to government decision-makers. This model remained workable so long as the objective was limited to the penetration and prevention of espionage and other long-term threats to the security of Canada. In retrospect, it is almost quaint to recall the UK’s traditional unwillingness to even acknowledge the existence of its security intelligence agencies.

He went on to

contrast this affinity for secrecy with the judicial system. The courts are traditionally grounded on principles of openness, transparency and public accountability. Fairness requires full disclosure of the case to be met, and public hearings before an independent, unbiased adjudicator. The rule of law, constitutionalism, and primacy of the rights of the individual are all salient features of this paradigm.

Intelligence agencies in the 21st century operate in a much more transparent manner than they did in the 1980s. For example, the British domestic security service, MI5, not only has a website, but the website recognizes that Security Service officers have testified in criminal trials involving terrorism and that, subject to valid claims of public interest immunity, intelligence may have to be disclosed in terrorism prosecutions. Mr. Sims’ comments, like those of the Supreme Court in Charkaoui II, reflect a growing appreciation that it is no longer realistic to imagine that security intelligence will never have to be disclosed in

---

57 Khawaja I, id., at paras. 145-147.
legal proceedings, especially legal proceedings involving allegations of terrorism as opposed to espionage. Changes in Canada’s legal and threat environment mean that secret intelligence will increasingly also be evidence or other material that may have to be disclosed in legal proceedings that attempt to detain, deport or punish suspected terrorists.

III. THE COURT’S DECISION IN KHADR

The Supreme Court’s decision in Khadr is best known for its decision that the Charter applied to the activities of CSIS officers who interviewed Omar Khadr at Guantanamo Bay, Cuba. My focus here will not be on the reasons why the Court held that the Charter had extra-territorial application, but rather on the disclosure of intelligence collected by CSIS. As will be seen, however, the two issues are not easily separated because the ambit of disclosure was limited by the Court’s understanding of the nature of the Charter and international human rights breaches that required the extra-territorial application of the Charter.

Omar Khadr was captured in Afghanistan when he was 15 years of age. He has been detained at Guantanamo Bay Cuba since October, 2002. His legal status has changed with the various changes in the legal regime that governs those detained at the American military base, but Mr. Khadr now faces charges of murder, attempted murder conspiracy, support of terrorism and spying under the Military Commissions Act.61 If convicted, Khadr could face life imprisonment and could potentially have faced the death penalty but the American government has decided not to seek a death sentence.

As explained in a recent decision finding that Khadr’s section 7 rights had been violated by the Canadian government’s continued refusal to request his return to Canada, “the events surrounding Mr. Khadr’s arrest in July 2002 are disputed. Clearly, he was present during a gun-battle near Khost, Afghanistan, during which a United States soldier was killed by a grenade. Mr. Khadr is alleged to have thrown the grenade. He maintains that he did not.”62 No allowance was made for Khadr’s youth and he was initially denied consular access at Guantanamo. CSIS agents

---

interviewed Khadr at Guantanamo while aware that he had been subjected to a so-called “frequent flier” program of sleep deprivation.63

1. The Case for Broad Disclosure Rights

Given the serious nature of the charges faced by Khadr, the harsh conditions of his confinement and the fragmentary and disputed nature of the evidence in his case, he had a strong case when he requested from the Canadian government full disclosure of all documents possessed by the Crown, including records of the interviews that Canadian officials conducted with Khadr at Guantanamo. Although the judge of first instance found that there was not enough of a causal connection between Canadian investigative actions and the American proceedings against Khadr, the Federal Court of Appeal reversed this decision and held that the Crown’s broad disclosure obligations under Stinchcombe applied in this case, subject to valid privilege or national security confidentiality claims that might be made by the Crown.

Justice Desjardins stressed the breadth of disclosure and stated that

[a] failure to disclose relevant information impedes an accused’s ability to make full answer and defence and creates the risk of an innocent person being convicted and imprisoned. As one of the principles of fundamental justice, the right to make full answer and defence has been entrenched in the section 7 protection of the right to life, liberty and security of the person.64

The Federal Court of Appeal decided this case before the Supreme Court placed new restrictions on the extra-territorial application of the Charter in R. v. Hape.65 It concluded that Khadr could receive full disclosure without interfering with the sovereignty of the United States because it would be up to the Americans to decide if any of the evidence was admissible in their own proceedings and to devise their own discovery process. The Federal Court of Appeal also recognized that the Attorney General of Canada could claim national security confidentiality before any actual disclosure was made.66

63 Id., at para. 17.
65 Supra, note 18.
66 Khadr v. Canada, supra, note 64, at paras. 36, 42.
The Supreme Court initially seemed to articulate a broad right to disclosure when it stated:

Canada has an obligation under s. 7 to provide disclosure to Mr. Khadr to mitigate the effect of Canada’s participation by passing on the product of the interviews to U.S. authorities. It is not clear from the record before this Court if all portions of all of the interviews were given to U.S. authorities. If Mr. Khadr is given only partial disclosure of the interviews on the ground that only parts of the interviews were shared with U.S. authorities, it may be impossible for him to evaluate the significance of the parts of the interviews that are disclosed to him. For example, by analogy with Stinchcombe, disclosure of an inculpatory statement shared with the U.S. authorities might require disclosure of an exculpatory statement not shared to permit Mr. Khadr to know his jeopardy and prepare his defence. It would seem to follow that fairness requires disclosure of all records in any form of the interviews themselves — whether or not passed on to U.S. authorities — including any transcripts, recordings or summaries in Canada’s possession. For similar reasons, it would seem to follow that Mr. Khadr is entitled to disclosure of information given to U.S. authorities as a direct consequence of Canada’s having interviewed him.67

In this passage, the Court seemed to endorse a broad approach to disclosure that borrows from its refusal in Stinchcombe to draw a distinction between the need to disclose inculpatory or exculpatory material. The Court in Stinchcombe68 recognized that what material was exculpatory could depend on the perspective of the participant and for that reason endorsed a broad rule that all relevant information be disclosed. The wisdom of this rule has been affirmed by subsequent work on tunnel vision and confirmation bias which suggests that investigators filter much of the information that they collect through cognitive biases that interpret evidence as consistent with the suspect’s guilt and resist classifying information as exculpatory. The Supreme Court was thus correct to suggest that even if only inculpatory material was shared with the United States, “fairness requires disclosure of all records in any form of the interviews themselves”69.

67 Khadr (S.C.C.), supra, note 3, at para. 34.
68 Supra, note 7.
69 Khadr (S.C.C.), supra, note 3, at para. 34.
2. Limiting Disclosure to the Scope of the International Human Rights Breach

Having suggested a rationale for broad disclosure patterned on Stinchcombe, the Court resiled from the principle that Stinchcombe would apply directly to CSIS even though such an approach had been endorsed by the Federal Court of Appeal. The Court reasoned that:

Our holding is not based on applying Stinchcombe directly to these facts. Rather, as described above, the section 7 duty of disclosure to Mr. Khadr is triggered on the facts of this case by Canadian officials’ giving U.S. authorities access to interviews conducted at Guantanamo Bay with Mr. Khadr. As a result, the disclosure order we make is different in scope than the order of the Federal Court of Appeal. The appellants must disclose (i) all records in any form of the interviews conducted by Canadian officials with Mr. Khadr, and (ii) records of any information given to U.S. authorities as a direct consequence of Canada’s having interviewed him. This disclosure is subject to the balancing of national security and other considerations as required by ss. 38 ff. of the Canada Evidence Act.\(^\text{70}\)

The Court reiterated the idea that disclosure was limited to the two categories articulated above in a subsequent part of the decision.\(^\text{71}\) The rationale for this restrictive approach seems to be that only information derived from the interviews at Guantanamo would constitute a violation of international human rights law and the Charter that required extra-territorial application of the Charter, something that has been seen as extraordinary after the Court’s decision in R. v. Hape.\(^\text{72}\) In this way, the Court’s restrictive approach to the extra-territorial effect of the Charter limited and narrowed disclosure rights and obligations under section 7 of the Charter.

Although the scope of the disclosure requirements in Khadr were limited by the extent of the Charter violation, it is significant that the disclosure obligations applied to information that was collected for intelligence purposes. Justice Mosley addressed this issue in his subsequent decision by noting:

Questions have arisen in these proceedings as to whether the visits had a law enforcement aspect, about which there is some dispute between the Attorney General and Mr. Khadr’s counsel. The former Deputy

\(^{70}\) Id., at para. 37 (emphasis added).

\(^{71}\) Id., at para. 40.

\(^{72}\) Supra, note 18.
Director of Operations for CSIS was cross-examined on the point in the course of earlier proceedings. From what I have seen, it appears clear that the interviews were not conducted for the purpose of assisting the US authorities with their case against Mr. Khadr or for building a case against him in Canada. I note that no law enforcement personnel were authorized to attend at that time. The information collected during the interviews was provided to the RCMP for intelligence purposes. However, it is equally clear that the US authorities were interested in having Canada consider whether Khadr could be prosecuted here and provided details about the evidence against him to Canadian officials for that purpose. Nonetheless, the interviews by Canadian officials were conducted for intelligence collection and not evidence gathering.

The Court’s ruling in this respect affirms the principle that intelligence may be subject to disclosure even if the intelligence was not collected for law enforcement purposes. This should dispel any residual ideas in CSIS that the organization is exempt from disclosure obligations because it does not have a statutory mandate to collect evidence. That said, disclosure of intelligence is far from automatic and CSIS will have an ability under section 38 of the Canada Evidence Act to obtain non-disclosure orders. One discipline on the breadth of the non-disclosure orders in criminal cases, namely, the ability of the trial judge to stay proceedings or order other remedies to the extent that the accused’s right to a fair trial is infringed, will not be present in Omar Khadr’s case if he is not subject to trial in Canada.

3. Subsequent Proceedings Reveal the Truncated Disclosure Obligation

In subsequent proceedings in the Federal Court to determine the exact extent of disclosure, Mosley J. recognized that there was some ambiguity in the Supreme Court’s approach to disclosure. He stated that “at first impression”, the Court’s reference to the Stinchcombe principle of disclosing all relevant information without regard to what was actually passed on to American authorities “would appear to leave open the possibility that the designated judge could apply a Stinchcombe relevance test to the redacted documents in the collection”. However,
he ultimately held that the disclosure obligation was limited to the two categories of records of the interviews of Khadr by Canadian officials and records of any information given to the Americans as a direct consequence of the Canadian interview. Thus, Mosley J. concluded that “the field of inquiry conducted by this Court has been considerably narrowed” and did not include “information in the collection which may have been considered relevant to the criminal charges under Stinchcombe” that had been “provided by U.S. agencies for intelligence and law enforcement purposes unrelated to the visits by Canadian officials to Guantanamo”. 76

The result of this narrowing exercise was that only five of 186 pages of interview notes and witness statements fell within the Supreme Court’s order even though all 186 pages would be relevant under Stinchcombe disclosure principles. 77 Thus the limited ambit of the extra-territorial application of the Charter established the limits for the disclosure. Stinchcombe relevant material that was unrelated to the Guantanamo interviews was not subject to disclosure even though such material was shared with the Americans and might have been relevant and useful to Omar Khadr in his defence.

Although Mosley J.’s subsequent ruling on the scope of the disclosure is based on an accurate and careful reading of the Court’s judgment, it is difficult to escape the conclusion that the result is to undercut the idea that fairness required broad disclosure to enable Khadr to better prepare his defence. Causation principles have limited the disclosure requirement because the disclosure requirement only applies to information about Khadr shared with the Americans “as a direct consequence of Canada’s having interviewed him”. This restrictive approach discounts Khadr’s interests in knowing all the information that Canada shared with the United States in order to better defend itself. To be sure, such information should not be disclosed if it was not relevant to the charges faced by Khadr or was subject to a valid privilege claim. These are matters that Mosley J. could have determined by reviewing the file with the help of arguments from the Attorney General of Canada and the security-cleared special counsel. Nevertheless, Mosley J. found that such a review of the whole file was not necessary because the Supreme Court had categorically limited the ambit of disclosure by requiring that the disclosure obligations would be limited to information obtained from

76 Id., at para. 29.
77 Id., at paras. 83-84.
the interviews or shared with the Americans as a result of the interviews and no more. In short, disclosure was limited to reflect the extent of the Charter and international human rights violation that required extra-territorial application of the Charter.

4. The Workability of Broader Disclosure Requirements

The restrictive nature of the Court’s disclosure obligations in *Khadr* discounts the work that relevance and privilege could do in ensuring that Khadr only gained access to CSIS information that would be relevant to his defence and would not be excessively damaging to Canada’s national security and international relations interests. For example, information that CSIS shared with the Americans about the activities of the Khadr family after Omar Khadr’s capture and detention would arguably not be relevant to his defence of the charges that he faced in American proceedings. Such a finding would have protected any ongoing investigations into other members of the Khadr family.

Most of the attention in cases and commentary has been paid to the breadth of *Stinchcombe* disclosure obligations, but there are limits to these obligations. For example, in 1995 the Supreme Court ruled that an accused could not have access under *Stinchcombe* to wiretaps that may have involved the accused on unrelated charges.\(^78\) In the follow-up proceedings from the Supreme Court’s decision in *Khadr*, Mosley J. recognized limits to *Stinchcombe* when he stated:

> It must be stressed that much of the redacted information in the documents produced to the Court does not relate to the applicant and would not assist him in defending himself against the criminal charges at Guantánamo. A considerable amount of this information refers to investigations concerning other persons unrelated to the applicant. This information would be irrelevant under the *Stinchcombe* standard.\(^79\)

Even if information shared with the Americans but unrelated to the Canadian interviews at Guantánamo had satisfied *Stinchcombe* requirements of relevance, the Attorney General of Canada would still have the opportunity to claim national security confidentiality privilege over such documents. The dominant test under section 38 is one that generally defers to the Attorney General’s claims that the disclosure of information would harm national security or international relations and

---

79 *Khadr v. Canada II*, supra, note 73, at para. 68.
requires the applicant to demonstrate that the harms of non-disclosure clearly outweigh the harms of disclosure.\textsuperscript{80} Indeed, the Supreme Court in the \textit{Khadr} case recognized the important safeguard that section 38 provides to the government of Canada to prevent disclosure of otherwise secret material with respect to the more limited category of material that was directly related to the Guantanamo interviews when it stated:

it is not possible on the record before this Court to determine what specific records should be disclosed to Mr. Khadr. In order to assess what specific documents must be disclosed as falling within the group of documents described in para. 37, a designated judge of the Federal Court must review the documents. The designated judge will also consider any privilege or public interest immunity claim that is raised, including any claim under ss. 38 ff. of the \textit{Canada Evidence Act}.\textsuperscript{81}

As noted above, the Federal Court of Appeal had applied the broader \textit{Stinchcombe} standard of disclosure, but also had reserved the ability of the government to justify selective non-disclosure under section 38 of the \textit{Canada Evidence Act} or other privileges.\textsuperscript{82}

In subsequent proceedings in this case, Mosley J. applied section 38 of the \textit{Canada Evidence Act}, which allows a designated judge to balance the competing interests in disclosure and non-disclosure of the information and concluded that the appropriate balance would require some editing of the videotapes of the interview of Khadr by Canadian officials at Guantanamo. The editing would prevent disclosure of the facial images of the Canadian officials and the disclosure of certain sensitive information that was not revealed in the public judgment. Justice Mosley concluded:

\begin{quote}
I am satisfied that disclosure of the sensitive audio content and the facial images would cause injury to Canada’s national interests and that there is no public interest in the disclosure of this information that outweighs the interest in non-disclosure. I have been advised that the DVDs could be edited to remove the audio containing the sensitive information and the identities of the officials/agents could be obscured. With those measures taken, any potential injury that might result from release of the tapes to Mr. Khadr’s defence team would be mitigated.\textsuperscript{83}
\end{quote}

\begin{footnotes}
\item[81] \textit{Khadr (S.C.C.)}, supra, note 5, at para. 38.
\item[82] \textit{Khadr v. Canada}, supra, note 64, at para. 42.
\item[83] \textit{Khadr v. Canada II}, supra, note 73, at para. 81.
\end{footnotes}
Similar measures could presumably have been taken if the Court had applied full *Stinchcombe* disclosure obligations.

5. Disclosure Only for Citizens?

One final restriction on the disclosure obligations articulated in *Khadr* is that they seem to be restricted to Canadian citizens even though section 7 of the Charter and *Stinchcombe* include non-citizens. The reference to Khadr’s citizenship was made by the Federal Court of Appeal in its ruling in the case which, as discussed above, held that *Stinchcombe* would apply and was made before the Supreme Court restricted the extra-territorial application of the Charter in *Hape*. In a subsequent decision about two other detainees held at Guantanamo and alleged to have been interviewed by CSIS and RCMP officials in 2003 and 2004, the Federal Court has distinguished the Supreme Court’s decision in *Khadr* on the basis that the applicants were not Canadian citizens. Justice Blanchard concluded “the Court is not prepared to extend the Charter’s reach beyond that which has already been decided. The Applicants are not Canadian citizens. They have failed to establish the required connection to Canada. Consequently their circumstances cannot engage a section 7 Charter right.” This is another example of disclosure rights being limited by the extent of the Charter’s extra-territorial application.

6. The Tensions Between *Khadr* and *Stinchcombe* and *Singh*

Although the Court’s decision in *Khadr* has resulted in some disclosure of intelligence to Omar Khadr, it is limited by the restrictions that the Court placed in *Hape* on the extra-territorial application of the Charter. Indeed, the *Hape*-inspired limitations in *Khadr* have created tensions with two landmarks in earlier section 7 jurisprudence: *Singh* and *Stinchcombe*.

---

85 *Khadr v. Canada*, supra, note 64, at para. 37.
87 Supra, note 18.
88 Supra, note 84.
89 Supra, note 7.
Khadr is in tension with Stinchcombe because the disclosure obligations in the former case are much narrower than Stinchcombe’s requirement that all relevant and non-privileged material be disclosed to the accused. The Court in Khadr does not reject the application of Stinchcombe on the basis that the proceedings that Omar Khadr faces in the United States are not criminal or will not result in severe consequences for Mr. Khadr. Such an approach would run counter to the Court’s recognition in other cases including Charkaoui II\(^9\) that section 7 is not limited to criminal proceedings and that some administrative proceedings in the anti-terrorism realm may have more severe consequences than criminal proceedings. Indeed, the likelihood that Khadr will not be subject to an ordinary criminal prosecution with its traditional safeguards makes the need for disclosure even more compelling.

The court rejects Stinchcombe disclosure rights in Khadr because it sees disclosure not as a right but as a remedy that is limited and defined by the extent of a Charter and international human rights violation that requires the extraordinary extra-territorial application of the Charter. As suggested above, such restrictions on disclosure can only be explained with reference to Hape. Moreover, they are unfortunate and unnecessary because the Stinchcombe limits of relevance and privilege would have given the government an ample opportunity to justify selective non-disclosure of material to Khadr.

By introducing the novel concept that section 7 rights are enjoyed only by Canadian citizens, Khadr also stands in tension to a long line of section 7 decisions starting with Singh which stress that section 7 rights are enjoyed by everyone and not just by Canadian citizens. Here again the only likely explanation for this doctrinal innovation seems to found in the Hape-inspired idea that courts must be cautious and restrictive in applying the Charter in an extra-territorial manner. The result may be that only Canadian citizens can claim the benefits of the extraordinary extra-territorial application of the Charter. Even accepting the need to establish some nexus to Canada, the citizenship category is a blunt and at times arbitrary one. A permanent resident may in some cases have a closer nexus to Canada than a citizen. In any event, limiting disclosure to citizens is in tension to the reference to everyone in section 7 of the Charter and the Charter’s relatively sparing use of citizenship as a category that defines the ambit of Charter rights.

\(^9\) Supra, note 4.
In the end, *Khadr* is something of a hollow victory for disclosure and section 7 of the Charter because it limits the scope of section 7 rights and of disclosure through its *Hape*-inspired understanding of the extraordinary nature of extra-territorial application of the Charter. *Khadr* limits key section 7 concepts of broad disclosure rights and universal personhood even while it finds that section 7 has been violated and CSIS intelligence should be disclosed given the particular and limited circumstances in which CSIS participated in a violation of Omar Khadr’s rights under international human rights law and the Charter. The message to CSIS seems to be that intelligence obtained abroad may have to be disclosed, but only to the extent that CSIS violates international human rights in a manner that requires the extra-territorial application of the Charter. The message to Omar Khadr is that the Court recognizes that his Charter rights were violated by CSIS participation in an international human rights violation, but that he will only receive disclosure of information that can be causally connected to the violation. Moreover, the government can still oppose such limited disclosure for reasons of national security confidentiality.

IV. THE COURT’S DECISION IN *CHARKAOUI V. CANADA*

The issue in *Charkaoui* was whether a person subject to a security certificate had a right to obtain notes of interviews conducted with him by CSIS in 2002. Adil Charkaoui was told that disclosure was impossible because the original notes had been destroyed pursuant to CSIS policy once the CSIS officers had completed their analytical reports. Mr. Charkaoui argued that he was entitled to the notes and a stay of proceedings or release as an appropriate remedy. He also asked that new evidence introduced by the Minister in 2005 be excluded. He received none of these remedies from the courts, but the Supreme Court did affirm that CSIS had a statutory and constitutional duty to retain and disclose the notes of their interviews with him.

1. The Trial Judgment

Justice Noël of the Federal Court rejected Charkaoui’s argument that his rights had been violated and that he was entitled to a remedy under the Charter. His judgment stressed that security certificates were not
criminal proceedings and that CSIS was not a police agency subject to disclosure obligations. He concluded that there was

no breach of procedural fairness as defined in section 7 of the Charter, the facts and allegations in the present proceeding not being based on these summaries. Nor, for the same reasons, is it necessary to discuss the role of CSIS in the investigation, other than to say that CSIS is not a police agency and that it is not its role to lay charges. As such, it cannot be subject to the same obligations as those attributed to a police force. Moreover, we are dealing here with immigration law, not the criminal law. The standpoint is different: see Blencoe v. British Columbia (Human Rights Commission), [2000] 2 S.C.R. 307, at para. 88, in which Mr. Justice Bastarache, on behalf of the majority, states: “This Court has often cautioned against the direct application of criminal justice standards in the administrative law area. We should not blur concepts which under our Charter are clearly distinct.” See also Canada (Minister of Employment and Immigration) v. Chiarelli, [1992] 1 S.C.R. 711; R. v. Lyons, [1987] 2 S.C.R. 309.91

Justice Noël’s 2005 decision was consistent with the idea articulated by the Pitfield Committee and discussed in the first part of this paper that stressed the distinctions between proactive and secret security intelligence and reactive and public policing. It also seemed to rely on the Court’s 1992 decision in Canada (Minister of Employment and Immigration) v. Chiarelli92 for the proposition that the security certificate process was consistent with the Charter even if it did not allow any adversarial challenge to the intelligence that the Ministers submitted in secret ex parte hearings to justify the issuance of the security certificate. This idea was rejected by the Supreme Court in its first Charkaoui decision in 2007.93

2. The Supreme Court’s Recognition of CSIS’s Evolving Role

The Supreme Court, in a unanimous judgment by LeBel and Fish JJ., allowed Charkaoui’s appeal and held that subject to editing by the reviewing judge, Charkaoui should have access to the original interview notes. The Court took a much more nuanced approach to the stark contrast between policing and security intelligence work than that taken

91  Re Charkaoui, supra, note 54, at para. 17 (F.C.).
93  Supra, note 23.
in 1983 by the Pitfield Committee or by Noël J. in the decision that was the subject of the appeal. For example, the Court stated:

Indeed, CSIS is not a police force. This is clear from the legislative history set out above. In reality, however, it must be acknowledged that the activities of the RCMP and those of CSIS have in some respects been converging as they, and the country, have become increasingly concerned about domestic and international terrorism. The division of work between CSIS and the RCMP in the investigation of terrorist activities is tending to become less clear than the authors of the reports discussed above seem to have originally envisioned.

. . . .

In this light, we would qualify the finding of the Federal Court that CSIS cannot be subject to the same duties as a police force on the basis that their roles in respect of public safety are, in theory, diametrically opposed. The reality is different and some qualification is necessary.\footnote{Charkaoui II, supra, note 4, at paras. 26, 28.}

The Court, through reference to the Arar Commission Report, took judicial notice of the changed circumstances in which CSIS operates especially since the events of September 11. In this context, it is no longer realistic or practical for CSIS to rely on the idea that intelligence must always remain secret or that it does not collect evidence. Although the jurisdictions of CSIS and the RCMP have from the start overlapped at least with respect to terrorist conspiracies, the enactment of many new terrorism offences in the 2001 \textit{Anti-Terrorism Act} has increased the degree of overlap.

3. CSIS’s Policy to Destroy Raw Intelligence

The Court considered a CSIS policy that required the destruction of operational notes. The rationale for the policy was the confidential nature of intelligence operations and the harm to national interests and affected persons that could be caused by the disclosure of intelligence. The only exception in the CSIS policy to the destruction policy was when retention of the original information was necessary because information such as a sketch or diagram could not be transcribed into an analytical report and when the information “may be crucial to the investigation of an unlawful act of a serious nature and employees may require their
notes to refresh their memories prior to recounting the facts of an event”.

The CSIS policy was first adopted in December 1994 and had been subject to only minor changes since that time. The CSIS policy was consistent with a Cold War mentality that valued secrecy above almost all other competing values. Although the policy made some allowance for the possibility that CSIS officers might have to testify in some serious terrorism prosecutions, it did not contemplate that CSIS officers would have to testify and present their work product in security certificate proceedings.

4. Section 12 of the CSIS Act

The Court found that the CSIS policy was based on an erroneous reading of section 12 of the CSIS Act. Section 12 is a critical component of the CSIS Act, but one that has received little if any judicial scrutiny. It provides:

The Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada.

Section 12 restricts collection of intelligence by CSIS by requiring that the investigation relate to “activities that may on reasonable grounds be suspected of constituting threats to the security of Canada” as defined in section 2 of the CSIS Act. Even where such a reasonable suspicion exists, section 12 places a further restraint that CSIS only collect information “to the extent that it is strictly necessary”. The reference to strictly necessary in section 12 follows recommendations made by the McDonald Commission that a civilian security intelligence agency should respect principles of proportionality in the collection of intelligence so as to avoid the excesses of the RCMP’s Security Service, which collected intelligence about opposition political parties and other forms of legitimate and lawful dissent in a democracy.

Although the “strictly necessary” qualifier seems in both a grammatical and purposive sense to qualify the reference in section 12 to

---

95 Id., at para. 35.
96 Id., at para. 30.
the collection of intelligence and not its subsequent retention or analysis, there was some ambiguity about the proper interpretation of section 12. For example, CSIS’s policy requiring the destruction of operational notes except in very limited cases might have been supported by arguments that the retention as well as the collection of intelligence should be limited by the “strictly necessary” qualification. The Supreme Court decisively rejected this argument in *Charkaoui II* by stating:

Nothing in this provision requires CSIS to destroy the information it collects. Rather, in our view, s. 12 of the *CSIS Act* demands that it retain its operational notes. To paraphrase s. 12, CSIS must acquire information to the extent that it is strictly necessary in order to carry out its mandate, and must then analyse and retain relevant information and intelligence. In short, OPS-217 rests on an erroneous interpretation of s. 12.97

The Court then proceeded to give a number of purposive or functional justifications for its interpretation of section 12 of the CSIS Act as requiring the retention of properly collected information. One justification was the need for precision and accuracy in intelligence as stressed by the Arar Commission in connection with its findings that inaccurate intelligence about Maher Arar and his wife had been shared with the Americans. Justices LeBel and Fish stated that:

The original operational notes will be a better source of information, and of evidence, when they are submitted to the ministers responsible for issuing a security certificate and to the designated judge who will determine whether the certificate is reasonable. Retention of the notes will make it easier to verify the disclosed summaries and information based on those notes. Similarly, it is important that CSIS officers retain access to their operational notes (drafts, diagrams, recordings, photographs) in order to refresh their memories should they have to testify in a proceeding to determine whether a security certificate is reasonable — a proceeding that is not mentioned in OPS-217.98

In this way, the Court noted that security certificates made use of intelligence as evidence and that such evidentiary uses of intelligence would require CSIS to adjust their retention policies to observe evidentiary standards.

---

97 *Id.*, at para. 38.
98 *Id.*, at para. 39.
5. Section 7 of the Charter

The Court interpreted section 12 of the CSIS Act in light of section 7 of the Charter and the security certificate context in which Adil Charkaoui asked for disclosure of the notes taken of CSIS interviews with him. Building on a theme expressed in its first Charkaoui case, the Court rejected the idea that section 7 rights were confined to the criminal justice system. Instead, the Court stated:

But whether or not the constitutional guarantees of section 7 of the Charter apply does not turn on a formal distinction between the different areas of law. Rather, it depends on the severity of the consequences of the state’s actions for the individual’s fundamental interests of liberty and security and, in some cases, the right to life. By its very nature, the security certificate procedure can place these rights in serious jeopardy, as the Court recognized in Charkaoui. To protect them, it becomes necessary to recognize a duty to disclose evidence based on s. 7.

The Court then took note that CSIS investigations “play a central role in the issuance of a security certificate” and that “the consequences of security certificates are often more severe than those of many criminal charges”. The context of the case made the need to retain the original notes pressing.

The Court also stressed the importance of retaining original notes so that both the Ministers who issue security certificates and the judges who review the reasonableness of the certificates would have an opportunity to verify CSIS’s analysis and conclusions against the original data. Justices LeBel and Fish stated:

As things stand, the destruction by CSIS officers of their operational notes compromises the very function of judicial review. To uphold the right to procedural fairness of people in Mr. Charkaoui’s position, CSIS should be required to retain all the information in its possession and to disclose it to the ministers and the designated judge. The ministers and the designated judge will in turn be responsible for verifying the information they are given.

100 Charkaoui II, supra, note 4, at para. 53.
101 Id., at para. 54.
102 Id., at para. 62.
The Court returned to the theme of verification when in the course of holding that Ministers could submit new evidence to support the security certificate, the Court stated that “receiving new evidence in the course of this ongoing verification process is fairer, since such evidence can be as beneficial to the named person as to the ministers”. The importance of verifying the conclusions and analysis of intelligence analysts will be discussed in the last part of this paper. With respect to section 7 of the Charter, however, the Court’s emphasis on verification is also supported by other section 7 jurisprudence which recognizes the possibility of error and unreliable evidence that can result in the detention of innocent persons.

6. Is Charkaoui II Based on Section 12 of the CSIS Act and/or Section 7 of the Charter?

The ultimate decision by the Court with respect to the duty to retain and disclose the original notes is a product of statutory interpretation of section 12 of the CSIS Act as influenced by the values of section 7 of the Charter and the principles of procedural fairness. The Court made reference to Charter values even though it did not recognize there was an ambiguity when the statute was interpreted in a purposive manner as required by cases such as Bell Express Vu Limited Partnership v. Rex.

Although the decision may be stronger by being supported by multiple legal sources, the amalgam nature of the ruling makes the decision less clear than it might have been. There may be a tendency in some quarters to read the decision narrowly as limited to the security certificate context that engages section 7 of the Charter and particular concerns about the procedural fairness of the decisions made by Ministers and reviewing judges in that process. Such an approach would, however, discount the Court’s interpretation of section 12 of the CSIS Act which applies to all of CSIS’s intelligence-collection activities. In this vein, it is important to reiterate that the Court said that the reference to intelligence in section 12 refers not only to “summaries prepared by officers” but also to “original operational notes” that are a “better source

---

103 Id., at para. 73.
of information, and of evidence”\textsuperscript{106} than the analytical summaries. Moreover, the Court clearly stated that nothing in section 12 “requires CSIS to destroy the information it collects. Rather, in our view, section 12 of the \textit{CSIS Act} demands that it retain its operational notes. To paraphrase section 12, CSIS must acquire information to the extent that it is strictly necessary in order to carry out its mandate, and must then analyse and retain relevant information and intelligence”\textsuperscript{107} The Court’s decision that CSIS should retain intelligence was rooted in section 12 of the CSIS Act and it would be a mistake to limit the Court’s holding to the security certificate process that engaged liberty and security interests under section 7 of the Charter.\textsuperscript{108} For example, the Court cited a decision by SIRC that had complained about the destruction of original notes in the context of a denial of a security clearance to Mr. Liddar. It also cited the Arar Commission with respect to the importance of accuracy and precision when intelligence is shared with other countries.\textsuperscript{109} Both of these contexts have nothing to do with security certificates. The Court’s interpretation of section 12 of the CSIS Act should apply across the board to all of CSIS’s activities and not be limited to the security certificate context.

Other agencies involved in the security certificate process such as the Canadian Border Service Agency and Immigration Canada, however, should take note of the Court’s comments about the importance of retention and disclosure of information given that the “consequences of security certificates are often more severe than those of many criminal charges”\textsuperscript{110} Even without the statutory re-enforcement of section 12 of the CSIS Act, those agencies may in some contexts have an independent obligation under section 7 of the Charter to retain and disclose relevant information to security certificate detainees. In short, there are two independent legal theories that support the conclusion that material must be retained for possible disclosure: the Court’s interpretation of section 12 of the CSIS Act and its interpretation of the requirements of section 7 of the Charter and closely related notions of procedural fairness. Both theories applied on the facts of \textit{Charkaoui II}, but each separate theory on

\begin{itemize}
\item \textsuperscript{106} \textit{Charkaoui II}, supra, note 4, at para. 39.
\item \textsuperscript{107} \textit{Id.}, at para. 38.
\item \textsuperscript{108} \textit{Id.}, at para. 50. The holding that s. 7 applied to the security certificate process was not novel and followed the Court’s prior decisions in \textit{Suresh}, supra, note 99 and \textit{Charkaoui I}, supra, note 23.
\item \textsuperscript{109} \textit{Charkaoui II}, id., at paras. 40-41.
\item \textsuperscript{110} \textit{Id.}, at para. 54.
\end{itemize}
its own could support a conclusion that material should be retained for possible disclosure.

7. **Privacy and the Distinction Between General and Targeted Investigations**

Although the Court interpreted section 12 of the CSIS Act to authorize the retention of properly collected intelligence, the Court did not deal directly with the restrictions that section 12 places on the collection of intelligence. This is unfortunate because a likely response to the Court’s decision will be that CSIS will retain much more raw intelligence. Indeed, modern computer technology would potentially allow CSIS to retain massive amounts of raw intelligence in excess of the prior holdings of the RCMP’s Security Service which were criticized by the McDonald Commission and civil libertarians.  

The Court was not completely oblivious to privacy values in *Charkaoui II* and it observed:

> The argument based on the importance of protecting privacy applies primarily to general investigations. Where targeted investigations are concerned, the interests at stake differ. Privacy should of course be respected, but not to the point of giving inaccurate or unverifiable information to the ministers and the judge. In the context of the procedures relating to the issuance of the security certificate and the review of its reasonableness, it may prove necessary to disclose notes to the ministers and the designated judge.  

The Court’s implicit assumption seems to be that the main danger to privacy comes from “general investigations” that do not involve named individuals and groups. Hence, the duty to retain intelligence does not apply in such investigations.

The Court’s concern that general investigations pose a threat to privacy makes intuitive sense. For example, a CSIS investigation into certain forms of political or religious activity or dissent could result in the investigation of those who were only engaged in legitimate activity or dissent or those who may have simply associated for social, economic, religious or political reasons with an individual or group that could be a

---

111 For a concrete example of some of the material collected and retained by the RCMP’s Security Service, see “Former RCMP Security Service Files on René Lévesque Now Available”, containing numerous press clippings and some heavily redacted material. Online: <http://wwwcollectionscanada.gc.ca/whats-new/013-314-e.html>.  
112 *Charkaoui II*, supra, note 4, at para. 44.
legitimate target of a CSIS investigation. In addition, the need to retain intelligence to promote adjudicative fairness is less pressing because enforcement actions ranging from the denial of a security clearance, to the issuance of a security certificate or a criminal prosecution are unlikely to result from a general investigation that does not focus on a specific individual or group.

Although it recognized that privacy concerns could still be in play with respect to targeted investigations of specific individuals and groups, the Court concluded that in such cases the balance of interests differed. In other words, concerns about accurate decision-making and adjudicative fairness favoured the retention of the original intelligence over the values of privacy. The need to retain accurate information in targeted investigations would also presumably extend to specific persons who were not targets of the investigation. For example, Maher Arar became a person of interest in an investigation of another target. A person denied a security clearance might have an interest in knowing what others said about him or her. Leaving aside the possibility that CSIS might target persons who are not legitimate targets because, for example, they simply engage in political or religious dissent, there is a possibility that the retention of information about those who associate with legitimate targets will adversely affect their privacy.

The distinction that the Court relies upon with respect to general versus targeted investigations raises the question of how CSIS actually conducts its investigations. Unfortunately, there is limited public information about CSIS’s targeting practices. The 2005-2006 annual report of the Security Intelligence Review Committee contains some interesting information about the authorized targets of CSIS investigations. In that year, there were 594 authorized targets, with 335 of the targets being for counter-terrorism and 192 being for counter-intelligence. Only 40 of the 594 authorized targets were identified as “issues/events” as opposed to individuals or organizations. If the Court in Charkaoui II was making reference to this distinction, it appears that more than 90 per cent of CSIS’s targeted investigations relate to individuals and groups. Such investigations would then engage the duty to retain and possibly disclose intelligence articulated in Charkaoui II. It is possible, however, that the Court was distinguishing between all targeted investigations, including those perhaps that target issues and events as opposed to

113 SIRC Annual Report, supra, note 26, Table 3, at 23. Unfortunately, similar data is not included in the 2006-2007 or 2007-2008 annual SIRC reports or in the CSIS annual reports.
individuals and organizations, and the other activities in which CSIS engages, such as open source research and the like. In either event, these figures suggest that the exemption of general investigations from the duty to retain and disclose may do little work in protecting privacy.

A finding that CSIS devotes most of its investigations to targeted individuals or groups is not a criticism of CSIS’s targeting decisions. Given limited resources and the risks of targeting legitimate dissent when one focuses on issues and events, it may be proper for CSIS to focus on specific individuals and groups who may be involved in activities that threaten the security of Canada. The targeting of events and issues could in some cases raise concerns about targeting legitimate political dissent or religious activity. The main point is simply that the Court may have (1) underestimated that the vast majority of CSIS investigations appear to target specific individuals and groups; and (2) overestimated the extent to which the exemption of “general” investigations from the duty to retain intelligence will protect privacy. If this is indeed the case, it will be very important for CSIS and its review bodies to ensure that targeting decisions are made carefully and legally, because once a group or an individual is targeted, it is now likely as a result of Charkaoui II that the raw intelligence on that person will be retained indefinitely. 114

8. Privacy and the Limits on Collection of Intelligence in Section 12 of the CSIS Act

Fortunately, there are some restrictions in the CSIS Act that are designed to protect privacy. Section 12 of the CSIS Act instructs CSIS that it shall collect information and intelligence with respect to “activities that may on reasonable grounds be suspected of constituting threats to the security of Canada”. In this way, CSIS must demonstrate that there is a reasonable suspicion related to threats to the security of Canada as defined in section 2 of the CSIS Act. The structure of section 12 of the CSIS Act follows the recommendations of the McDonald Commission, which stressed the importance of a statutory definition of the mandate of a new civilian security intelligence in order to ensure that the new agency respected legitimate dissent in a democracy and to ensure that its activities were subject to the rule of law.

114 The Court does not address how long intelligence should be retained and there may be a case for legislation or regulation to address this issue which will also involve the related issue of the preservation of CSIS records for archival historical research.
Even when CSIS is investigating reasonably suspected threats to the security of Canada, section 12 of the CSIS Act places an additional restriction on its activities: information and intelligence are to be collected “to the extent that it is strictly necessary”. The reference to necessity follows recommendations made by the McDonald Commission that the activities of a new civilian security intelligence agency should be guided by principles of proportionality. Principles of proportionality have subsequently played an important role under the Charter, most notably in relation to the justification of reasonable limits on Charter rights under section 1 of the Charter. There is little jurisprudence that illuminates either the meaning of threats to the security of Canada as defined in section 2 of the CSIS Act or the precise nature of the “to the extent that it is strictly necessary” limitation in section 12 of the CSIS Act. The Supreme Court in Charkaoui II did not attempt to fill this gap or to flesh out how restrictions in section 12 of the CSIS Act should govern the collection of intelligence, which under its ruling is now likely to be retained by CSIS for much longer periods. The Court’s failure to do so is unfortunate because it would have naturally flowed from its discussion of privacy and the retention of intelligence. Although some defend minimalist rulings in the national security area,\(^{115}\) national security issues are rarely litigated\(^{116}\) and the Court can provide important guidance in the few that are litigated.

Given the possible adverse effects that increased retention of intelligence could have on privacy values, it would have been helpful for the Court to have provided some guidance about the proper interpretation of the rest of section 12 of the CSIS Act, particularly as it related to the collection of intelligence. Although section 12 is the centre piece of the CSIS Act and has been in place for a quarter of a century, there still has been no definitive judicial interpretation of when activities are reasonably suspected of being a threat to the security of Canada or when the collection of intelligence is strictly necessary to investigate such threats.\(^{117}\) In the absence of such guidance from the Court, much of the work in defining the limits of its mandate will fall on CSIS and review bodies such as SIRC and the Privacy Commissioner. The increased


\(^{117}\) Section 12 has been interpreted as not authorizing extra-territorial searches: see Re X, 2007 Carswell Nat 5260.
retention of intelligence that will be promoted by *Charkaoui II* makes it only more important that the intelligence be legally and properly collected in the first place.

9. **What Should Be Disclosed and to Whom?**

As in *Khadr*, the disclosure authorized in *Charkaoui II* was far from absolute. The Court at several junctures noted that the reviewing judge would still be obliged under the *Immigration and Refugee Protection Act* not to disclose to Charkaoui any material that if disclosed could harm national security or endanger any person.\(^{118}\) Indeed this standard is more restrictive than the standards under section 38 of the *Canada Evidence Act* that were applied in *Khadr* and would be applied in cases arising from *McNeil*\(^ {119}\) that may require the disclosure of CSIS information in terrorism prosecutions. Under section 38 the designated judge is allowed to balance and reconcile the competing interests in disclosure and non-disclosure whereas under the *Immigration and Refugee Protection Act* that designated judge is absolutely prohibited from disclosing any information to the detainee that would harm national security or any individual. In reality, this means that much of the intelligence in security certificate cases that is subject to disclosure under *Charkaoui II* will be disclosed to the security-cleared special advocates created in the wake of *Charkaoui I* and not to the actual detainees and their lawyers.

Although *Khadr*, *Charkaoui II* and *McNeil* all send definite and important signals to CSIS about the need to retain original intelligence and its possible disclosure in subsequent legal proceedings, all of the decisions recognize that disclosure will not be absolute. All three decisions provide the government an opportunity to justify non-disclosure on grounds relating to harms to national security. In the security certificate context, it is likely that a significant amount of the raw intelligence will not be disclosed to the detainee on the basis that its disclosure would harm national security or other persons, including those who have collected the intelligence. In such instances, the raw intelligence

---

\(^{118}\) *Charkaoui II*, supra, note 4, at paras. 45, 63, 77.

\(^{119}\) *Supra*, note 6. CSIS information could be subject to disclosure in a terrorism prosecution on the basis (1) that CSIS was an investigating agency directly subject to *Stinchcombe*; (2) that the Crown knew about prior CSIS investigations and had a duty to seek and disclose relevant information or; (3) on the basis that the evidence was truly relevant in the criminal trial even if CSIS is classified as a third party not directly subject to *Stinchcombe*. The Court in *McNeil* recognizes that disclosure can be prevented in all three scenarios by a valid claim of privilege.
will be disclosed to the special advocate, who must then obtain judicial permission in order to consult the detainee or others when necessary to make inquiries about the context in which the raw intelligence was collected.

The disclosure of more raw intelligence to the special advocates will likely result in more requests by special advocates to presiding judges to allow them to contact the detainees about the meaning and accuracy of the raw intelligence. It may also lead the special advocates to seek permission from the judge to share the raw intelligence with intelligence experts who can opine on the meaning and reliability of the raw intelligence and whether it supports the analytical conclusions drawn from it by CSIS and others. Although the Court stresses the value of the retention of the raw intelligence in allowing Ministers and reviewing judges to verify the analytical conclusions drawn by CSIS, this process will be assisted by the adversarial challenge that has been promoted by the special advocates created in the wake of Charkaoui I.

10. Remedies for Failure to Retain and Disclose Intelligence

Although CSIS should respond to Charkaoui II by changing its policy to destroy intelligence, the immediate challenge in many security certificate and other proceedings may be to devise remedies for the failure to disclose raw intelligence that CSIS has already destroyed. As discussed above, Adil Charkaoui sought both the exclusion of evidence and a permanent stay of proceedings as remedies for CSIS’s failure to retain and disclose intelligence in the form of the original notes of interviews with him.

The Court rejected the request for a stay of proceedings stressing that the stay should be “a remedy of last resort”120 and that it was premature to issue such a drastic remedy while the proceedings were ongoing. The Court also noted that the designated judge had granted an appropriate remedy when he had postponed proceedings in response to late disclosure in 2005 of the summary of CSIS interviews with Charkaoui in early 2002.121 This approach is consistent with the Court’s restrictive approach in criminal cases with respect to granting stays of proceedings

---

120 Charkaoui II, supra, note 4, at para. 76.
121 Id., at para. 67.
as a Charter remedy.\textsuperscript{122} The Court only briefly adverted to its own extensive jurisprudence on breaches of the duty to retain evidence that has been developed in the criminal context\textsuperscript{123} and it warned about the need for a contextual approach. CSIS’s destruction of intelligence in targeted investigations after the Court’s decision in \textit{Charkaoui II} will likely be found to be unacceptable negligence under \textit{R. v. La.}\textsuperscript{124} The issue of whether there was unacceptable negligence may have to be litigated in the many cases where the intelligence was destroyed before \textit{Charkaoui II}. In a sense, Charkaoui was given the retroactive benefit of the Court’s ruling in his case as is the general rule in litigation.\textsuperscript{125}

The task of devising an appropriate remedy was delegated to the reviewing judge who would hear evidence from those who took the interview notes. Given that much relevant intelligence will likely have already been destroyed pursuant to CSIS policy in \textit{Charkaoui} and the other security certificate cases, the task of devising appropriate and just remedies under section 24(1) of the Charter for any section 7 violations caused by the destruction of relevant intelligence will only add to the already onerous litigation that surrounds the use of security certificates based on allegations of involvement with terrorism. In some cases, the presiding judge may have to exclude evidence of intelligence conclusions if the raw intelligence that is necessary to verify the conclusions has been destroyed.

The Court in \textit{Charkaoui II} left some room for judges in other cases to find that a failure to disclose relevant intelligence did not violate section 7 of the Charter or section 12 of the CSIS Act when it warned that the duty of retention was not absolute, and that “while it is true that CSIS officers routinely take notes, they doubtless do not prepare accurate transcripts of their interviews with the individuals they are investigating. Finally, important information may go missing as a result of simple human error.”\textsuperscript{126} Although these scenarios are possible, it is likely that, as in \textit{Charkaoui II}, much raw intelligence in ongoing cases will have been deliberately destroyed pursuant to CSIS policy. It is also likely that allegations of a failure to disclose relevant intelligence and requests for remedies for that failure will become a staple of litigation in the ongoing

\textsuperscript{122} See Kent Roach, \textit{Constitutional Remedies in Canada} (Aurora: Canada Law Book, 2008), as updated ch. 9.
\textsuperscript{123} \textit{Charkaoui II}, supra, note 4, at para. 49.
\textsuperscript{126} \textit{Charkaoui II}, supra, note 4, at para. 45.
security certificate cases. When the raw intelligence has been retained, it may also be necessary for the special advocate to ask permission from the judge to consult with others to understand the full significance of the intelligence and its reliability. Such litigation will add to the already daunting complexities of security certificate cases, again raising the issue of the sustainability of such procedures.127

V. SOME IMPLICATIONS OF KHADR AND CHARKAOUI II AND THE “JUDICIALIZATION OF INTELLIGENCE”

The Supreme Court’s decisions in Khadr and Charkaoui II, when combined with the Court’s even more recent decision in McNeil, send a clear signal to CSIS that its intelligence holdings are not exempt from disclosure. In light of these rulings, CSIS should no longer rely on the simplistic idea that it does not collect evidence or that CSIS agents should destroy original notes or raw intelligence in order to ensure the secrecy of such intelligence. Although the combined effects of these rulings do not make CSIS a police force, they do move CSIS closer to the practices of police officers with respect to the collection and retention of original information. In this way, the rulings are part of the judicialization of intelligence identified by CSIS Director Jim Judd a few months before the release of Khadr and Charkaoui II.

A complex phenomenon such as the judicialization of intelligence will have both positive and negative effects. Some likely effects of this process will be outlined below before an initial judgment is made. Any such judgment should be tentative because the process of the judicialization of intelligence remains dynamic. It is dependent on how CSIS, those affected by CSIS intelligence and the courts respond to the possibility revealed in Khadr and Charkaoui II that more CSIS intelligence will be subject to disclosure in legal proceedings.

127 For other arguments that security certificates are not sustainable in the terrorism context, see Kent Roach, “Khadr and Bill C-3: Some Implications for Anti-Terrorism Policy and Dialogue Between Courts and Legislatures” (2008) 42 S.C.L.R. (2d) 281 [hereinafter “Roach, “Khadr and Bill C-3””].
1. Possible Harms of the Judicialization of Intelligence

(a) Disclosure of Legitimate Secrets?

One possible harm of the judicialization of intelligence is that it could result in the disclosure of secret information that will harm confidential sources and methods used by CSIS and allied intelligence agencies. One oft-cited example of such harms is a report that Osama bin Laden stopped using a satellite phone following press reports that such calls were being monitored by American intelligence agencies. The exact accuracy of these claims has recently been questioned, but the possibility that the judicialization of intelligence could lead to disclosure of material that should be kept secret cannot be ignored. This is especially the case given Canada’s oft-noted reliance on intelligence provided by foreign agencies.

Claims that the Supreme Court in Khadr and Charkaoui II has been insensitive to CSIS’s demands for secrecy cannot, however, be sustained. In a number of cases, the Supreme Court of Canada has recognized that CSIS has legitimate secrets to keep and that many of these secrets are on loan from foreign agencies who apparently provide Canada with most of its intelligence. The Supreme Court did not actually order that intelligence be disclosed in either Khadr or Charkaoui II. Instead the Court ordered that further proceedings be held to determine what evidence should be disclosed. In Khadr, these proceedings involved a specially designated judge of the Federal Court balancing competing interests in disclosure and non-disclosure under section 38 of the Canada Evidence Act. In Charkaoui II, the designated judge would be required by the Immigration and Refugee Protection Act not to disclose any information to the detainee that would harm national security or any person. In both cases, the Court made generous allowance for the protection of legitimate secrets. The same is true of the more recent McNeil case where the Court recognized that a successful claim of privilege, such as informer privilege or the national security confidentiality privilege under section 38 of the Canada Evidence Act,

---

129 Charkaoui I, supra, note 23; Ruby v. Canada (Solicitor General), supra, note 23.
130 The judicialization of intelligence may also produce attempts to create new privileges to shelter intelligence from disclosure. For a recent decision recognizing a privilege for CSIS sources that is subject to a “need to know” principle, see Re Harkat, [2008] F.C.J. No. 1823, 306 D.L.R. (4th) 269 (F.C.).
could prevent disclosure of relevant information either under \textit{Stinchcombe} \footnote{Supra, note 7.} or under the third party procedures articulated in \textit{O’Connor}. \footnote{Supra, note 9.}

It appears unlikely that cases such as \textit{Khadr} or \textit{Charkaoui II} will result in the disclosure of intelligence that will harm ongoing national security investigations or the lives of vulnerable sources. If a judge, however, makes a mistake and orders too much disclosure, the Attorney General of Canada can issue a non-disclosure certificate under section 38.13 of the \textit{Canada Evidence Act} to prevent disclosure under that section. The options are a bit less clear if too much disclosure is ordered under the \textit{Immigration and Refugee Protection Act}. Under that Act, judges are instructed not to disclose any information that would harm national security or endanger any person and they are not allowed to balance the competing interests in disclosure and non-disclosure. In some cases, it may be possible for the government to stop disclosure by withdrawing those parts of its allegations that make the disclosure relevant. In an extreme case, the Court could prevent disclosure by abandoning the security certificate proceeding.

\textbf{(b) Creating False Confidence in the Accuracy of Intelligence?}

Another possible danger is that the retention of raw intelligence to allow for verification and adversarial challenge may suggest that intelligence is actually more reliable than it is. The process of verification and adversarial challenge will only be as accurate and reliable as the underlying data. The fact that intelligence after \textit{Charkaoui II} may be verified against the raw intelligence will not necessarily mean that the intelligence itself is reliable or accurate. It is also possible that adversarial challenge of the intelligence will fail to reveal inaccuracies in the intelligence.

Although the above dangers are real, they would exist with or without the judicialization of intelligence that is contemplated in the retention and disclosure of raw intelligence. Such retention and disclosure will at least allow security-cleared special advocates an opportunity to provide innocent explanations for raw intelligence that might on its face confirm suspicions. It should also allow for challenges to the methods that were used to obtain the raw intelligence, especially in...
cases where methods used abroad may potentially adversely affect the reliability of the intelligence. The ability of the special advocate to challenge the raw intelligence may in some cases require the special advocate to be able to consult with the detainee or others after having seen the raw intelligence.\footnote{Such consultations after the special advocate has seen the secret information would have to be authorized by the judge under s. 85.2(c), as amended, to respond to \textit{Charkaoui I}, supra, note 23. For discussion of this section, see Roach, “\textit{Charkaoui and Bill C-3},” \textit{supra}, note 127, at 315-17.} A refusal to allow the special advocate to engage in such consultations could impair that person’s ability to challenge the intelligence and could increase the chance that unreliable intelligence will wrongly be perceived as reliable.

There is a danger that retention and disclosure of the raw intelligence may create a false confidence in intelligence that may have been selectively collected and may not be reliable. That said, the danger of overly filtered or unreliable intelligence would persist even in the absence of cases such as \textit{Charkaoui II}. The retention and disclosure of the raw intelligence at least provides some opportunity for verification and adversarial challenge.

\subsection*{(c) Increased Retention of Intelligence as a Threat to Privacy?}

The most serious danger of a judicialization of intelligence that results in increased retention of raw intelligence is its potential threat to privacy. \textit{Charkaoui II} could promote a process that Stanley A. Cohen has referred to as “dossier building” where intelligence, including dubious intelligence based on rumours, associations and unsubstantiated suspicions, is retained perhaps permanently on file or more likely in an accessible electronic database.\footnote{Stanley Cohen has argued that given its emphasis on the risk of future harm rather than concrete events, “an intelligence dossier will naturally contain a range of information, including much that is unsifted or unfiltered, as well as innuendo, hearsay and speculation. … The intelligence practices of the national security world would encourage the amassing of detailed information for possible future linkage. This leads to dossier building and the creation of generalized suspect lists.” Stanley A. Cohen, \textit{Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril} (Markham, ON: LexisNexis Canada, 2005), at 404.} It would technologically be possible for CSIS to retain far more files on individuals than the former Security Service of the RCMP, which was criticized by the McDonald Commission for the extensive files that it held on many Canadians, including some who were participating in legitimate forms of dissent and even some in minority political parties such as the Parti Québécois and the New Democratic Party.
A possible answer to these privacy concerns, however, can be found in CSIS’s mandate and its review structure. Section 12 of the CSIS Act restricts the collection of intelligence to that which is strictly necessary to investigate reasonably suspected threats to the security of Canada as defined in section 2 of the Act. Unfortunately, the Court did not elaborate on the meaning of this part of section 12 in its decision in Charkaoui II. This was a missed opportunity by the Court to flesh out how the concept of reasonable suspicion, recognized in other parts of the law, applies to CSIS’s investigations of threats to the security of Canada. Moreover, the Court could also have explored how principles of proportionality articulated by the McDonald Commission and in its own section 1 jurisprudence might have informed and disciplined the requirement that even in cases of reasonably suspected threats to the security of Canada, CSIS should only collect intelligence to the extent that it is strictly necessary for the investigation. These are critical parts of section 12 of the CSIS Act that the Court could have interpreted in response to the legitimate concerns that it discussed that CSIS’s increased retention of intelligence could harm privacy.

Now that the Supreme Court has clarified that section 12 does not justify the destruction of raw intelligence, it will be even more important for CSIS and its review bodies to ensure that CSIS only collects intelligence pursuant to its lawful mandate. This is an important part of the project of subjecting CSIS to the rule of law. In this sense, Charkaoui II is only relevant to one part of the intelligence cycle, namely, the retention of raw intelligence that is the basis for CSIS’s analysis and conclusions. Given that raw intelligence is much more likely to be collected after Charkaoui II, it becomes even more important to ensure that the intelligence is properly and lawfully collected pursuant to CSIS’s mandate. This process would be facilitated if CSIS was able to provide more public information about its targeting process and if SIRC devoted more attention to this critical topic in its annual public reports about its review of CSIS.

2. Possible Benefits of the Judicialization of Intelligence

(a) Disclosure as a Means to Reveal Tunnel Vision and Other Errors in Intelligence?

The Court in Charkaoui II stressed that retention of the original notes or raw intelligence was required to ensure that both the Ministers and the reviewing judges could discharge their duties under the statutory scheme. In both cases, the Ministers and reviewing judges should have access to the original data and notes to ensure the accuracy of the analytical reports and conclusions that CSIS prepared.\textsuperscript{136} The Court recognized that the analytical reports prepared by intelligence agencies could be overstated or just plain wrong. If criminal trials can reach wrong conclusions about guilt or innocence, it should hardly be surprising that intelligence analysis which is conducted in secret and without adversarial challenge may also be wrong. Nevertheless, sensational but erroneous conclusions made by those who have secret raw intelligence — for example, conclusions that Maher Arar and his wife were associated with Al Qaeda or that five of the September 11 terrorists entered the United States from Canada\textsuperscript{137} — have an unfortunate way of sticking around long after the original data for such conclusions has been found to be lacking.

Lest it be thought that it is only lawyers who are concerned about the fallibility of intelligence, much of the writing by intelligence practitioners and scholars today accepts the possibility if not the inevitability that intelligence analysts will at times reach conclusions that are wrong, including some conclusions that are not supported by the underlying data. As Peter Gill and Mark Phythian, two leading intelligence scholars, have observed, intelligence “remains an intellectual process … However many ‘facts’ are compiled or integrated they still do not ‘speak for

\textsuperscript{136} Supra, note 4, at para. 62. The Court observed: As things stand, the destruction by CSIS officers of their operational notes compromises the very function of judicial review. To uphold the right to procedural fairness of people in Mr. Charkaoui’s position, CSIS should be required to retain all the information in its possession and to disclose it to the ministers and the designated judge. The ministers and the designated judge will in turn be responsible for verifying the information they are given. If, as we suggest, the ministers have access to all the undestroyed “original” evidence, they will be better positioned to make appropriate decisions on issuing a certificate. The designated judge, who will have access to all the evidence, will then exclude any evidence that might pose a threat to national security and summarize the remaining evidence — which he or she will have been able to check for accuracy and reliability — for the named person.

\textsuperscript{137} Andrew Mitrovica, “Former US spy linked 9/11 terrorists to Canada”, Toronto Star (April 24, 2009), A23.
A former CIA analyst has written that “in order to tell decisionmakers about what is going on overseas and who is doing it, intelligence analysts spend much of their time linking disparate data together to either ‘connect the dots’ or ‘create the mosaic’.” He adds that “because raw intelligence data … is usually fragmentary — providing an incomplete picture of what is actually going on overseas or in the mind of the adversary — the gaps in the data must be filled in with assumptions drawn from various sources, running from the theoretical literature to the analysts’ idiosyncratic judgment.” 139 Intelligence analysis is an inherently creative process, but it should be disciplined by the ability to check the analysis against the raw data. This is especially important when individuals will be harmed as a result of the intelligence analysis.

Recent and spectacular intelligence failures include the failure to connect the dots of September 11 and the false connection of the dots with respect to weapons of mass destruction in Iraq. Richard Betts has argued that intelligence failures are inevitable because of the ambiguity of much raw intelligence and the need for intelligence analysts to provide governments with workable advice. 140 Another former intelligence analyst for the CIA has stressed that “intelligence collection systems produce sensory data, not intelligence. Only the human mind can add the discernment and knowledge that makes sense of it. It is only after ‘raw’ data are verified for accuracy and evaluated for significance can they become the substance of intelligence.” 141

Richard Heuer Jr., who worked within the CIA from 1951 to 1979 and who retired as the head of the methodology unit in the Director of Intelligence’s political analysis office, has warned of the dangers of premature closure, selective perception of relevant facts, cognitive biases and not considering alternative hypotheses. 142 In what in the criminal justice context would be called tunnel vision, he has observed that “people do not naturally seek disconfirming evidence, and when such

---

evidence is received it tends to be discounted.” Heuer has warned that intelligence analysis is closer to the process of writing history than conducting scientific analysis. Another person who works in military intelligence has drawn on Heuer’s work to warn:

humans are prone to self-confirmation in cases where equivocal information exists or, in other words, ‘we perceive what we expect to perceive’. A wealth of research has demonstrated the human tendency to search out and attend only to evidence that confirms one’s ideas, beliefs, or hypotheses. The problem with the confirmatory tendency is that only information supportive of one’s beliefs is attended to, even in the face of extremely disconfirming information. Information that could provide corrective feedback that one’s beliefs are in error is rarely evaluated. This process of searching for confirmation can lead to some very inaccurate conclusions, and may lead to an increased, perhaps unjustified, confidence in one’s conclusions.

All of this analysis suggests that CSIS, as much as the Court, should be concerned about preserving raw intelligence so that it can verify the accuracy of its analytical intelligence.

The Court’s repeated references in Charkaoui II to the ability of Ministers and judges to verify intelligence against raw intelligence alludes to the increased recognition of the fallibility of the intelligence product. In this sense, the decision is very much influenced by the findings that the Arar Commission and SIRC respectively reached in the Maher Arar and Bhupinder Liddar cases that unsupported and erroneous conclusions had been drawn in the intelligence process in a manner that harmed these men. The Court’s decision is designed to allow the relevant decision-makers to review the raw data on which CSIS bases its analysis. Retention of the raw data increases the accountability of CSIS and provides a basis for a Minister or a judge to ask CSIS some very hard questions. That said, the check on CSIS is still limited by whether the raw intelligence has already been destroyed pursuant to the CSIS policy found deficient in Charkaoui II and by the reliability and relevance of the raw data itself.

---

143 Id., at 61.
144 Id., at 136.
(b) Increased Adjudicative Fairness?

The ultimate objective of the proceedings in Khadr and Charkaoui II is to increase the fairness of the proceedings that both men face. Omar Khadr’s ability to defend himself in American proceedings could potentially be improved by the disclosure of the interviews he had with CSIS officials and by information that CSIS shared with the Americans. The adequacy of the disclosure that Khadr will receive from American officials remains very much in doubt. 146 Unfortunately, the disclosure obligations articulated by the Supreme Court of Canada in his case are defined narrowly in a manner that mirrors the limited extra-territorial reach of the Charter. In other words, the Court has limited disclosure to information collected or shared with the Americans as a direct consequence of the Guantanamo interviews that implicated Canada in an international human rights violation. The disclosure obligations in Khadr do not extend to other Stinchcombe-relevant material that Canada possesses, including material that it has shared with the Americans that is not related to the interviews. These restrictions on disclosure impose real limits on how helpful the decision will be to Omar Khadr. A broader definition of what should be disclosed to Khadr would not have threatened legitimate secrecy interests because the government would still have been able to argue that the information was not relevant to the charges faced by Khadr and that the information was privileged by national security confidentiality. Such a tailored approach is better than imposing broad and categorical restrictions on disclosure that have the potential to deny important and even potentially exculpatory information to the accused.

The Court’s decision in Charkaoui II at first blush seems more generous to the affected person because it defines the disclosure obligations more broadly than Khadr. The Court in Charkaoui II was appropriately aware of the severe consequences of the security certificate process and the fact that section 7 of the Charter is not restricted to the criminal process. The Court in Charkaoui II laid to rest any idea that section 12 of the CSIS Act provides a statutory justification for the

146 A plurality of the United States Supreme Court in Hamdi v. Rumsfeld, 542 U.S. 507, 124 S.Ct. 2633 (2004) seemed to approve of significant departures from traditional criminal law standards of adjudicative fairness but the United States Supreme Court has subsequently found existing standards at Guantanamo Bay to be unconstitutional: Hamdan v. Rumsfeld, 548 U.S. 557, 126 S.Ct. 2749 (2006) and Boumediene v. Bush, 128 S.Ct. 2229 (2008). The dissenters in Boumediene, however, specifically complained that the majority had not dealt with issues such as disclosure when it declared that the Guantanamo detainees should have access to habeas corpus.
destruction of properly collected intelligence. At the same time, *Charkaoui II* did not actually order that the interview notes or other raw intelligence be disclosed to the detainee. Much of this material may already have been destroyed pursuant to CSIS policy. The Court rejected a stay of proceedings as a drastic and premature remedy for such destruction. Even to the extent that the material has been retained, the Court recognized that the judge would still have to filter out any material that if disclosed would harm national security or any person. To be sure, there are benefits in terms of adjudicative fairness in allowing Ministers, reviewing judges and security-cleared special advocates to see all the raw and available intelligence. At the same time, however, *Charkaoui II* may not dramatically increase the actual disclosure made to the detainee. Such conclusions are troubling for adjudicative fairness, but as discussed above, they also belie any claim that the Court has effectively opened CSIS’s vaults to public disclosure. The value of *Charkaoui II* in terms of adjudicative fairness may well depend on what the special advocates can do with the raw intelligence. As suggested above, special advocates may find it necessary to return to the detainee or others in order to assess the broader context and meaning of raw intelligence to which they may gain access under *Charkaoui II*.

(c) *Increased Accountability for CSIS?*

Disclosure of CSIS intelligence not only has the potential to increase the fairness of legal proceedings, but it can also provide a valuable accountability check on the accuracy, fairness and precision of the analytical conclusions that CSIS draws from its raw intelligence. The Court in *Charkaoui II* was influenced by Commissioner O’Connor’s finding that an analytical conclusion (admittedly made by the RCMP and not by CSIS) that Maher Arar and his wife were Islamic extremists associated with Al Qaeda was inaccurate. Full disclosure of the original intelligence is a necessary precondition to ensuring that the conclusions reached by intelligence analysts are fair, accurate and supported by the raw intelligence.

The Court seemed to believe that the Ministers of Public Safety and Immigration who decide to issue security certificates would be in a

---

147 For a recent recognition that a detainee’s rights may be threatened when the bulk of the government’s case is only disclosed to special advocates, see *A v. United Kingdom*, App. No. 3455/05 (2009) (European Court of Human Rights), at para. 220.
position to verify the intelligence provided by CSIS to justify the signing of a security certificate and to justify the maintenance of the security certificate process. Although the Ministers do have this responsibility, it is not clear how well they have discharged the responsibility given their other responsibilities and position within the government. The Ministers may be tempted to defer to CSIS’s expertise in evaluating intelligence, but they should now have access to all the relevant intelligence before they decide to sign a security certificate. It is also noteworthy that the Ministers have not signed a security certificate in a case with allegations of terrorism since they signed Mr. Charkaoui’s certificate in 2003.

The reviewing judge is in a better position than the Ministers to verify CSIS’s analysis against the raw intelligence. The reviewing judge may have or develop expertise in intelligence matters and the judge enjoys the protections of judicial independence. In addition, the judge should be assisted by adversarial arguments provided by detainees and special advocates that even the most diligent and expert Minister will not be able to access.

Although CSIS’s review body SIRC already should have access to all CSIS material, it should also benefit from Charkaoui II to the extent that the decision requires CSIS to retain the original intelligence it collects about specific individuals or groups. The Court quoted from a SIRC decision in the Liddar case that had expressed frustration with the fact that interview notes originally taken by CSIS in the course of a security clearance interview were unavailable. After Charkaoui II, SIRC, which has the statutory ability to see all information held by CSIS with the sole exception of Cabinet confidences, should be in a better position to verify CSIS’s analysis and conclusions against the raw intelligence. This is an important side benefit of the Court’s decision and again underlines that Charkaoui II has effects far beyond the security certificate context.

(d) Increased Cooperation Between CSIS and Law Enforcement?

The Court’s decision in Charkaoui II rejects the blunt and outdated idea that CSIS is not involved with the collection of evidence that was articulated by the Pitfield Committee in 1983 and reflected in the trial judge’s original decision that disclosure was not required because CSIS was not a police force or involved with the enforcement of the criminal

---

148 CSIS Act, s. 39.
law. In the late 1990s, the Security Intelligence Review Committee identified *Stinchcombe* and the fear of disclosure as a significant impediment to CSIS and RCMP cooperation. The trial judge in the Air India trial found that CSIS had violated section 7 of the Charter by its destruction of the Parmar wiretaps and the original notes of interviews with important witnesses. To the extent that the judicialization of intelligence represented by cases such as *Charkaoui II* requires CSIS to retain intelligence and to deal with the possibility that intelligence might be disclosed in legal proceedings, such a process should make it easier for CSIS to work with law enforcement.

Greater attention to evidentiary standards in the collection and retention of intelligence may be one of those happy scenarios where reforms can both improve the fairness of the process for those who may be accused of terrorism and improve the effectiveness of the system that society uses to prevent the very real dangers of terrorism. Such results, however, will depend on CSIS accepting the judicialization of intelligence process identified by Mr. Judd and promoted by *Khadr, Charkaoui II* and McNeil.

VI. CONCLUSION

The Supreme Court’s decisions in *Charkaoui II*, *Khadr* and *McNeil* are all consistent with the judicialization of intelligence thesis articulated by Jim Judd shortly before the release of those decisions. All three decisions send signals to CSIS that the intelligence that it collects may be subject to disclosure in subsequent proceedings. *Charkaoui II* is the most important of the decisions for CSIS because it finds that long-standing CSIS policies that required the destruction of raw intelligence are contrary to section 12 of the CSIS Act and, in the security certificate context at least, contrary to section 7 of the Charter. *Charkaoui II* represents a fundamental challenge to the way that CSIS has destroyed original intelligence in the name of secrecy.

Jim Judd did not really address whether the judicialization of intelligence was a positive or negative development. This is understandable given his position, but it will be important that CSIS not resist the trends that Mr. Judd has identified and that it not demonstrate too much

---

149 Supra, note 4.
150 Supra, note 3.
151 Supra, note 6.
attachment to or nostalgia for its long-standing policy of destroying raw intelligence. Some might argue that the judicialization of intelligence places legitimate and important secrets collected by CSIS and shared with CSIS by allied agencies at risk. At their crudest, such claims amount to attacks that lawyers and judges do not understand the security threats that Canada faces or the legitimate needs for secrecy to protect sources and CSIS’s relations with allied agencies. Such claims are difficult to sustain given the Court’s refusal in both Khadr and Charakouei II actually to order that intelligence be disclosed. In both cases, the government was given ample opportunity to justify to the courts the need for non-disclosure of sensitive intelligence. Some within intelligence agencies might object to having to convince judges of the need and justification for secrecy, but such objections are really objections to CSIS being subject to the rule of law. Such objections are inconsistent with the post-1982 rejection of absolute state prerogatives to assert unreviewable claims of secrecy.

Other weightier objections can be made against the judicialization of intelligence. One concern is that the process of verification of intelligence analysis against raw intelligence promoted by Charakouei II might create unwarranted confidence in the reliability and probative value of intelligence. The verification process that is promoted by Charakouei II can reveal some errors in intelligence analysis, but it should also be remembered that even verified intelligence will only be as accurate and precise as the original raw data. The collection of the raw data may be skewed and the raw data may be wrong or unreliable. Even when verified against raw intelligence, intelligence of the sort that is used to support security certificates may still remain much less reliable than evidence. Intelligence may be obtained from foreign agencies in circumstances that are not conducive to respect for human rights. Intelligence may, as in the case of Maher Arar and other Canadians held abroad, be based on false confessions made to avoid torture or mistreatment. Intelligence linking persons to terrorism could be verified against the original raw intelligence, but the intelligence could still be wrong if the original information was a false confession or misinformation. In many cases, little may be known about how foreign agencies obtained the information and so the reliability of the intelligence will not be clear. Intelligence can be based on untested and untestable hearsay, including rumour and reputation evidence. It may view ambiguous behaviour and associations through an interpretative lens that can make the agency’s predictions about security threats
something of a self-fulfilling prophecy. The retention of intelligence under Charkaoui II provides some potential correctives, but intelligence, even when verified against the raw intelligence that has been collected, will remain fallible.

The most serious concern about Charkaoui II is that it could lead to increased retention of massive amounts of raw intelligence in a manner that will threaten privacy. CSIS could respond to Charkaoui II by retaining everything it collects in the vast majority of its targeted investigations. Although the Court was not oblivious to privacy concerns, its limitation of the duty to retain intelligence to investigations that target individuals and groups is no real limitation if over 90 per cent of CSIS targeted investigations still target specific groups and individuals as opposed to general causes and events. CSIS’s mandate means that it should generally target individuals and groups because the targeting of events and causes is less discriminating and can catch more legitimate dissent. Nevertheless, the targeting of individuals and groups, combined with the duty to retain intelligence in Charkaoui II, modern information technology and the expanded resources that CSIS has received since September 11, means that CSIS could collect and retain a staggering amount of intelligence. Given this, CSIS and its review bodies must pay close attention to restrictions on its ability to collect intelligence and it is unfortunate that the Supreme Court in Charkaoui II did not address how section 12 of the CSIS Act restricts CSIS to the collection of intelligence that is strictly necessary to investigate reasonably suspected threats to the security of Canada.

Although Charkaoui II presents some dangers, its potential benefits are great. Increased retention of intelligence may play a role in helping CSIS work better with law enforcement. This has the potential to benefit both society through more effective investigations and prosecutions and the accused to the extent that the intelligence collected and retained by CSIS may assist the accused in his or her defence. CSIS like police forces must be reminded that it has a duty to look for and collect exculpatory as well as incriminatory material and it should follow the best thinking within intelligence agencies which recognizes the dangers of confirmation bias or tunnel vision in the collection and analysis of intelligence.

Increased disclosure obligations have the potential to increase the accountability of CSIS and to ensure that its analytical product is subject to full adversarial challenge. As the Court repeatedly stressed in Charkaoui II, the retention of raw intelligence provides an important
opportunity for both internal and external testing of the validity of CSIS’s analytical conclusions. Much recent writing about intelligence by intelligence scholars and practitioners recognizes the fallibility of the analysis process and to this extent Charkaoui II should not be dismissed by CSIS as a decision that imposes alien lawyers’ values on the security intelligence world. At the same time, Charkaoui II follows in the tradition of other section 7 decisions that have concerned themselves with the possibility of miscarriages of justice that harm the innocent.

The Court’s decision in Khadr to limit CSIS’s disclosure obligations to the extent to which the Charter would be applied extra-territorially in response to hopefully rare international human rights violations by Canadian officials, however, is unfortunate. Khadr limits the ability of disclosure to prevent intelligence errors and to provide accountability for CSIS’s extra-territorial work. This again reaffirms the need for review agencies to be given sufficient resources and powers to match the increased resources and powers given to intelligence and other agencies with national security responsibilities.

The ability of the judicialization of intelligence to produce increased adjudicative fairness for persons such as Omar Khadr and Adil Charkaoui remains to be determined. It is significant that the Court did not actually order the disclosure of intelligence in either case. The promise of disclosure in each case will require judges to resist any overclaiming of secrecy by the government. In the security certificate context, a significant amount of the raw intelligence may only be disclosed to special advocates. It will be important that special advocates have the necessary information from detainees and others to engage in full and informed adversarial challenge of the raw intelligence. To this extent the success of Charkaoui II may depend on the success of the reforms initiated by Charkaoui I.

As Jim Judd accurately predicted, the judicialization of intelligence is an important change and challenge for intelligence agencies. It is a process that is likely to continue in a post-Cold War environment where there is increased emphasis on counter-terrorism and the rights of those accused of involvement in terrorism. Given this, it will be best if CSIS accepts Charkaoui II and the duty to retain intelligence for possible disclosure, and abandons any nostalgia it may have for a world in which intelligence could be collected, analyzed, and destroyed so that it could be kept secret forever.
On July 8, 2009 and subsequent to the completion of this paper, the Security Intelligence Review Committee (SIRC) took the extraordinary step of publishing an unclassified report on CSIS’s involvement in the Omar Khadr case. This report provides independent confirmation of the phenomenon of the judicialization of intelligence identified by Jim Judd and discussed at length in this paper.

The SIRC report found that post-September 11 terrorism investigations have “blurred the line between the work of intelligence and law enforcement agencies, and thus between intelligence and evidence”. CSIS information is more frequently being used in legal proceedings and “intelligence that is found to have been gathered in circumstances that violated domestic laws or international conventions will not only be rendered useless in the courtroom, but more importantly, will bring discredit to the Service”.152 In other words, CSIS needs to respect evidentiary standards in its terrorism investigations both to preserve its own reputation and to ensure that it can cooperate with law enforcement agencies.

SIRC recommended that “CSIS can no longer carry out its mandate solely from an intelligence-gathering perspective. Political, judicial and legal developments post 9/11 are forcing the Service to take a less insular approach to its work and to consider various extra-intelligence factors”,153 most notably the need to respect human rights and evidentiary standards. It called on the Minister of Public Safety to provide guidance and advice to CSIS to help it “undertake a fundamental re-assessment of how it conducts business, and to undergo a cultural shift in order to keep pace with the political, judicial and legal developments of recent years”.154 As suggested in the first part of this paper, CSIS must abandon Cold War policies that maximized secrecy and rejected the idea that intelligence would ever be disclosed in legal proceedings.

153 CSIS’s Role, id., at 1.
154 Id., at 7.
In completing its important report, SIRC examined all hard copy and electronic documents held by CSIS relating to Omar Khadr between May 2002 and September 2005. It found no legal documentation of a legal opinion being obtained by CSIS before it questioned Omar Khadr for intelligence purposes at Guantanamo despite widespread reports of abuses at the military base at the time.\(^\text{155}\) It also found that the United States insisted as a condition of the visits that it record CSIS interviews with Omar Khadr,\(^\text{156}\) thus making the issue of information sharing that was the focus of the Supreme Court’s decision in Khadr somewhat academic. CSIS did, however, share its analytical reports from the Khadr interviews with American agencies, the RCMP and the DFAIT. CSIS maintains that the Khadr interviews produced undisclosed but “important intelligence gains” albeit ones that were “not particularly helpful in terms of offering new investigative leads”\(^\text{157}\).

SIRC criticized CSIS both for failing to obtain a legal opinion before interviewing Omar Khadr and for failing to take into account his position as a youth who “been kept incommunicado and been denied access to legal counsel, consular representation or family members”.\(^\text{158}\) SIRC also interpreted the Federal Court’s injunction which prevented further interviews at Guantanamo\(^\text{159}\) and the Supreme Court’s decision requiring disclosure of those interviews\(^\text{160}\) as a “message” from the courts that “CSIS can no longer undertake its activities solely through the insular lens of intelligence-gathering, rather it must consider the wider environment and implications within which its work is carried out. This includes both the Canadian Charter of Rights and Freedoms and Canada’s obligations under international law.”\(^\text{161}\)

The SIRC report is a helpful and influential confirmation of the growing judicialization of intelligence that is supported by the Charkaoui II,\(^\text{162}\) Khadr\(^\text{163}\) and McNeil\(^\text{164}\) cases discussed in this paper. It goes beyond Jim Judd’s recognition of the judicialization of intelligence as a phenomenon that is making CSIS’s work more difficult to argue that

\(^{155}\) Id., at 2, 4, 5.1, 5.2.

\(^{156}\) Id., at 4.1.

\(^{157}\) Id., at 4.2.

\(^{158}\) Id., at 6.


\(^{160}\) Khadr (S.C.C.), supra, note 3.

\(^{161}\) CSIS’s Role, supra, note 152, at 7.

\(^{162}\) Supra, note 4.

\(^{163}\) Supra, note 3.

\(^{164}\) Supra, note 6.
CSIS must move beyond its Cold War origins and should accept the increased accountability and fairness that come with the exposure of intelligence to disclosure in legal proceedings.