Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

TOP SECRET

File No.: 2800-157
(TD R508)

REVIEW OF CSIS'S INTELLIGENCE TO EVIDENCE PROCESS

(SIRC STUDY 2010-05)

Security Intelligence Review Committee
May 13, 2011

ATIP version
dated: MAR 2 0 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

TABLE OF CONTENTS

ATIP version
MAR 2 0 2019
dated:

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

EXECUTIVE SUMMARY

This review examines how CSIS is meeting the challenges posed by the growing use of security intelligence in criminal proceedings, using the Toronto 18 as a case study.

SIRC's review first looked at the framework governing cooperation between CSIS and the RCMP, as well as the approaches and tools that the Service, separately or in conjunction with the RCMP, has developed to manage this important relationship. SIRC found that significant progress had been made in this area, specifically, that CSIS and the RCMP have implemented a process that allows for effective cooperation, deconfliction and dialogue.

In recognition of the fact that discussions with respect to "intelligence to evidence" are ongoing, SIRC identified three issues that CSIS may want to examine more closely.

First, SIRC looked at the two-letter mechanism used by the Service to disclose information to law enforcement. SIRC recommends that, in order to improve the quality and value of the information CSIS provides to its law enforcement partners, and to bring consistency to the way in which CSIS discloses information to law enforcement, CSIS should adopt a one-letter disclosure model that espouses the standards of rigorous legal review currently set for advisory letters.

The second issue concerns verbal exchanges with law enforcement. Here, SIRC reminds CSIS of the importance to keep proper records of verbal exchanges, consistent with recent jurisprudence on the subject of retention, as well as the Service's own approach to retention.

The third issue for consideration related to the use of information obtained from CSIS warrants in criminal proceedings. SIRC wishes to impress upon the Service that, because the information that CSIS provides to other government departments and agencies is increasingly before the courts as part of criminal prosecutions and other court proceedings, the obligation to provide full, fair and frank disclosure of all material facts should be well understood by all CSIS employees.

SIRC found that the Toronto 18 case underscored the Service's ability to work with the RCMP in the new environment brought about as a result of the passage of the *Anti-terrorism Act*; however, the Service's approach to the "intelligence to evidence" challenge will continue to evolve as it receives guidance, both from the courts and the government.

ATIP version
dated: MAR 2 0 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

1 INTRODUCTION

Cooperation and information-sharing among members of the security and intelligence community have been a key feature of Canada's national security posture post 9/11. This issue was brought to the forefront with the passage of the *Anti-terrorism Act,* which resulted in CSIS and the RCMP becoming increasingly involved in investigating the same activities, "as activities related to terrorism can constitute both a threat to the security of Canada and a crime."[1] Indeed, in his inquiry into the investigation of the bombing of Air India Flight 182, Justice Major observed that there have been a growing number of cases where there has been pressure to disclose intelligence in criminal proceedings, a process that some have coined the "judicialization of intelligence."

CSIS has been wrestling to meet the challenges posed by this trend. In late 2007, the CSIS Deputy Director of Operations (DDO) assessed that "the current onslaught of civil suits, inquiries, judicial reviews, extraditions and criminal proceedings are presenting serious challenges to the protection of our ongoing investigations and assets"; he believed that even deeply-cherished assumptions that CSIS could protect its information, investigative methods

Shortly thereafter, the CSIS Director stated publicly that intelligence agencies have had to confront "a range of legal issues such as disclosure, evidentiary standards, and the testimony of intelligence personnel in criminal prosecutions," all of which have profound implications for the conduct of intelligence activities.[3] It is recognized that adjudication of these issues will be piecemeal, with judgments rendered in anti-terrorism prosecutions helping to shape CSIS's future strategy.

Chief among these cases is the "Toronto 18", the largest, and ultimately successful, terrorism investigation since the *Anti-terrorism Act* came into force. The investigation dates back to 2005, when CSIS was investigating a homegrown terror cell engaged in the "planning, and related preparatory stages, of an act of terrorism

it would later be revealed that this plot

---

1 In December 2010, the government announced *The Government of Canada Response to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182* that included initiatives aimed at improving the relationship between intelligence and evidence in criminal proceedings. For example, the government said it would "explore the process of disclosure and the obligations of Canada's security intelligence agencies [and] examine how security intelligence is collected and retained." The government will have a prominent role in elaborating, with the input of other stakeholders such as the Department of Justice and Public Safety, the appropriate whole of government response to the challenge of intelligence to evidence.

3 Remarks by Jim Judd at the Global Futures Forum Conference (Vancouver, April 15, 2008).

ATIP version
MAR 2 0 2019
ated:

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

involved storming Parliament Hill and detonating truck bombs in downtown Toronto. The severity of the threat led the RCMP Integrated National Security Enforcement Team (INSET) to launch its own investigation, known as Project Osage, in November 2005. For the next seven months, CSIS and the RCMP undertook "separate and distinct " investigations that culminated in the June 2006 arrests of 18 individuals on terrorism-related charges. Four adults and three youths had charges against them stayed; seven adults pleaded guilty, including the two ringleaders. The remaining four accused chose to fight their charges at trial - and all were convicted.[5]

Using the Toronto 18 as a case study, this review examines how CSIS has risen to the challenge presented by the increased use of security intelligence in criminal proceedings. This review sought to answer such fundamental questions as: What policies and processes are in place to enable CSIS intelligence to be used as evidence in court? How do CSIS and the RCMP cooperate while still respecting their respective roles in terrorism investigations? How has CSIS dealt with some of the challenges that have arisen from the use of intelligence in court proceedings? Have there been any "lessons learned", and if so, have any changes occurred in policy or practice?

The review first looks at the framework governing cooperation between CSIS and the RCMP, as well as the approaches and tools that the Service, separately or in conjunction with the RCMP, has developed to manage this important relationship. The review then examines the Toronto 18 investigation, focusing on how the Service and the RCMP handled cooperation in this investigation, before turning to a discussion of the two important rulings that emanated from the prosecutorial process and what those rulings mean for the Service. The final section consists of a discussion of several issues that warranted closer examination.

---

5 http://www3.thestar.com/static/toronto18/index.html

ATIP version
dated: MAR 2 0 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

2 METHODOLOGY

SIRC recognized at the outset of this review that it would be unable to examine all aspects of the issue of "intelligence to evidence", given its complexity and multifaceted nature. For this reason, SIRC picked the Toronto 18 investigation as a case study because it is one of the first major *Anti-terrorism Act* prosecutions in Canada that has worked its way through the criminal justice system. Although this methodology does not provide SIRC with a full picture of CSIS's efforts to address the "intelligence to evidence" challenge, it nonetheless provides an ideal "snapshot".

First, SIRC set out to examine how CSIS intelligence was collected and disclosed to the RCMP for use in the prosecution of the Toronto 18. To achieve this, SIRC undertook an in-depth review of CSIS's investigations against the group's two leaders, Fahim Ahmad and Zakaria Amara. SIRC looked at CSIS's operational reporting and exchanges with the RCMP, to understand the process that was followed with respect to cooperation and information-sharing on a groundbreaking anti-terrorism case. SIRC then assessed how this process stood up to legal scrutiny by examining all Ontario Superior Court decisions that emanated from this case, focusing on those that had implications for CSIS's role and actions.

In addition to a review of CSIS documentation, SIRC staff attended several briefings with senior CSIS personnel who were involved in the Toronto 18 case, both at the CSIS HQ and regional levels, as well as from the operational and litigation sections. These discussions enhanced SIRC's overall understanding of the key issues at play in the "intelligence to evidence" debate.

ATIP version
MAR 2 0 2019
dated:

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

3 CSIS-RCMP COOPERATION AT A GLANCE

The guiding principle underlying CSIS-RCMP cooperation is that each organization has a distinct mandate. The RCMP is a police force with policing authorities and duties; its main function is to mount investigations that lead to the prosecution of those who break the law. CSIS is an intelligence gathering agency whose mandate is to advise government about potential threats to national security. At the same time, the *CSIS Act* does recognize that the Service may come into possession of information that may be of value to law enforcement.[6]

Disclosing secret intelligence to law enforcement is fraught with difficulty, given the need to protect certain secret intelligence from disclosure in an open criminal prosecution. Far from being only a concern to CSIS, disclosure of secret intelligence to law enforcement carries risks for both parties. When secret information from the Service seeps into a police investigation, it will generally have to be disclosed. If disclosing that intelligence compromises the integrity of CSIS investigations or its tradecraft, the Crown may opt to terminate the prosecution, which is not a desirable outcome for law enforcement. For CSIS, disclosing intelligence-gathering methods or sources can impair its long term effectiveness. These risks were highlighted by the judge presiding over the Toronto 18 prosecutions, who recognized that "both organizations have a distinct interest in maintaining a degree of separation between their operations. Avoiding such problems is clearly in the public interest."[7]

3.1 The Framework for Cooperation

Section 19 of the *CSIS Act* stipulates that CSIS *may* share information with law enforcement[8], which according to CSIS, provides it with the "latitude" needed to protect "some ongoing investigations whereby there's absolutely no need to inform the RCMP."[9] Several reasons can explain why CSIS may choose not to disclose

---

6 Under s. 19(2)(a) of the *CSIS Act*, CSIS may disclose information "where the information may be used in the investigation or prosecution of an alleged contravention of any law of Canada or a province, to a peace officer having jurisdiction to investigate the alleged contravention [...]."

7 R. V. Ahmad et al., Ruling No. 14 (May 8th, 2009) Brampton CRIMJ(F)2025/07 (Ont. S.CJ) at paragraph 33.

8 The discretion that CSIS has in determining what to share with law enforcement has prompted criticism by some, including former Supreme Court Justice John Major, who argued that CSIS has too much discretion.

9 In fact, according to the submission of the Attorney General of Canada to the Major Commission, "a very minor portion of what CSIS investigates ever becomes relevant to a criminal investigation, even though 60-70% of CSIS' current work is in the field of

ATIP version
dated: MAR 2 0 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

information to law enforcement: some individuals operate just under the criminal law threshold; other individuals represent a threat to national security as a result of activities conducted abroad, sometimes in places where it would be difficult to gather evidence to support a criminal prosecution; and, finally, the third-party rule makes some intelligence received from foreign partners impossible to convert into "evidence". CSIS has asserted publicly that the system of information-sharing between CSIS and law enforcement "works well", and that both agencies "have developed credible and effective tools to ensure appropriate information is shared in a timely way."[10]

One such tool is the January 2010 Deputy Director Operations (DDO) Directive on *Disclosure of Service Information to the RCMP/Police and other Enforcement Agencies*, which states that decisions to share intelligence with the RCMP "should be grounded in an assessment of the nature and seriousness of the criminal activity which is suspected, and consideration of the potential impact sharing the information may have on the Service's investigations." The Directive also stipulates that CSIS should share information with the RCMP, in spite of the risk to the Service, based on "exigent circumstances." As CSIS explained, considerations of public safety trump disclosure risks; in other words, if CSIS found itself in a situation where it needed to share information on an imminent threat with the RCMP, it would do so, and resolve any disclosure issues later.[11]

The Service is also in the process of developing target management tools that will further support the disclosure process. These tools are intended to provide a framework through which to approach the issue of whether and when the Service should engage domestic partners in taking specific action on targets. This could involve, as examples, disclosing information to law enforcement in anticipation of a police investigation or to the Department of Citizenship and Immigration in the context of security certificates. SIRC considers this effort to inject more rigor into CSIS's decision-making processes with respect to disclosures a positive development.

Alongside these initiatives are joint CSIS-RCMP efforts to intensify ongoing cooperation, such as the development of a Joint National Counter Terrorism Strategy that identified a number of broad objectives to enhance the management of counter-

---

counter-terrorism. Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, "Final Submissions of the Attorney General of Canada, Volume I of III", paragraph 410.

10 Remarks by CSIS's Assistant Director of Intelligence, Ray Boisvert, to the Canadian Association for Security Intelligence Studies Conference (Ottawa, October 14, 2010).

11 SIRC Briefing on Disclosure and Cooperation with the RCMP, December 22, 2010.

ATIP version
dated: MAR 2 0 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

terrorism investigations.[12] In 2006, CSIS and the RCMP signed a new Memorandum of Understanding (MOU) that provides guidance with respect to the exchange of information and intelligence and the provision of operational support and assistance. This agreement stipulates that CSIS may , on a timely basis or upon request by the RCMP, provide information and intelligence in its possession that may assist the RCMP in fulfilling its national security-related responsibilities. In addition, the creation of the CSIS-RCMP Joint Management Team (JMT) has provided a mechanism through which to structure cooperation.[13] These initiatives support CSIS's current approach to information-sharing, which is to share information early and on an ongoing basis with the RCMP. This is reflected in the submission of the Attorney General of Canada to the Major Commission, which states that CSIS is disclosing "aggressively" to the RCMP to allow "the RCMP to satisfy itself as to whether a criminal threshold has been reached on a given CSIS file."[14]

These ongoing strategic discussions and coordination between the Service and law enforcement are important because they give the RCMP an opportunity to determine whether a CSIS investigation has met the required threshold for police to initiate their own criminal investigation. It also serves to keep both agencies current on any investigation of significance. Additionally, early coordination or "joint target management" has the potential to minimize disclosure problems by facilitating the timely launch of a police investigation.

In briefings with SIRC, CSIS officials also emphasized the importance of personal relationships and training in managing coordination and cooperation efforts with the RCMP. In Toronto Region, for example, SIRC was told that the relationship with the RCMP is very strong.

---

12 Specifically, the strategy committed to: better manage the RCMP-CSIS operational relationship on counter-terrorism issues; develop a new framework for pursuing criminal prosecutions; and review the legal framework implicated in using intelligence as evidence. Several specific initiatives were also included, such as developing joint training programs with the RCMP and developing a "joint case management" system. Joint National Counter Terrorism Strategy (RCMP MOU 200-12

13 The goals of the JMT are to ensure effective coordination of investigations through meaningful, timely and ongoing exchange of information, development of common counter terrorism threat overview and priorities and joint training initiatives

14 Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, "Final Submissions of the Attorney General of Canada, Volume I of III", paragraph 416.

ATIP version
dated: MAR 2 0 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Overall, SIRC sees the intensification of cooperation between CSIS and the RCMP and the development of tools to manage disclosure as positive developments. In this next section, we examine how this approach to cooperation was put to the test during the Toronto 18 investigation.

ATIP version
MAR 2 ? 2019
dated:

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

4 THE TORONTO 18 INVESTIGATION AND TRIAL

The RCMP commenced its Project Osage investigation in November 2005, following a CSIS Advisory Letter advising that Fahim Ahmad was believed to be a threat to national security. SIRC was told that the RCMP was able to get its own investigation up and running quickly; by the time the RCMP applied for a warrant one month after the investigation began,

The RCMP's ability to move forward quickly was greatly facilitated by the willingness of a crucial CSIS human source to work with police.

Following the start of Project Osage, CSIS continued its own investigation against several of the Toronto targets. Although CSIS's investigation focused on gathering intelligence to support its security intelligence mandate, and not for the purpose of gathering evidence, the extent of the overlap between the two agencies' investigations required a high degree of coordination. In general, CSIS made efforts to stay out of the way of the RCMP investigation to allow the police to gather evidence required for prosecution.

SIRC was told that during the Toronto 18 investigation, CSIS approached the issue of information-sharing with the RCMP with a great deal of circumspection. In several cases, CSIS was in possession of important information that was not shared with the RCMP out of concern that the Service would be construed as directing the RCMP investigation. As Justice Dawson commented, "...CSIS had to ensure that the RCMP got onto the right investigative path, without providing more information than was necessary to ensure that public safety was protected."[16] For example, a senior CSIS official from Toronto testified that "CSIS was aware of the location of the terrorist training camp that was to be held. This information was not provided to the RCMP, who had to uncover that information by their own means."[17] In another instance, "CSIS was aware that the RCMP were following the wrong target person, or that they had surveillance on a house when the target of the surveillance was not inside, but they did not intervene."[18] Communication and information-sharing nonetheless took place through frequent contact between senior RCMP and CSIS regional officials, who were

---

16 R. V. Ahmad et al., Ruling No. 14 (May 8th, 2009) Brampton CRIMJ(F)2025/07 (Ont. S.CJ) at paragraph 43.

17 R. V. Ahmad et al., Ruling No. 14 (May 8th, 2009) Brampton CRIMJ(F)2025/07 (Ont. S.CJ) at paragraph 43.

18 R. V. Ahmad et al., Ruling No. 14 (May 8th, 2009) Brampton CRIMJ(F)2025/07 (Ont. S.CJ) at paragraph 43

ATIP version
dated: MAR 2 2 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

mindful of the need to maintain their exchanges at a strategic level, and for CSIS not to compromise the police investigation by passing along detailed information. The RCMP also shared the fruits of its own investigation with CSIS for practical reasons, namely to give CSIS a sense of how the police investigation was progressing to avoid intelligence gaps, especially in the event that the police investigation ended abruptly.[19]

SIRC was told that the Toronto 18 investigation was ideal, in that it was possible to move cautiously and deliberately in order to maintain the strict separation between CSIS and the RCMP. This pace facilitated the "highly controlled" manner in which the Service proceeded, something that turned out to be critical to the favourable rulings.[20] In this next section, we examine two judgments rendered by the Ontario Superior Court of Justice in the course of the Toronto 18 trials that focused on the Service's cooperation and information-sharing practices with the RCMP.

4.1 "Separate and Distinct"

The first key ruling, delivered in May 2009, concerned the question of whether CSIS and the RCMP maintained separate pursuits of their respective mandates throughout the investigation. The accused asserted that CSIS had to be considered "an other investigating state authority"[21] and therefore subject to full disclosure. The Crown and CSIS argued that CSIS had to be regarded as a third party for disclosure purposes, arguing that CSIS conducted a separate investigation in accordance with its national security mandate.

In his ruling, the judge concluded that the RCMP and CSIS maintained "separate and distinct" investigations, the effect of which was to spare CSIS from the same full disclosure of its investigation as the police. As evidence, the judge pointed to the fact that CSIS did not "direct" the RCMP investigation, and to the tightly controlled flow of information from CSIS to the RCMP. As already noted, although the RCMP shared the results of its investigation with CSIS on an ongoing basis, CSIS only occasionally

---

19 To facilitate this, there was a CSIS officer embedded in the INSET who was responsible for ensuring that CSIS received all the detailed operational information related to the RCMP investigation. This officer did not share CSIS information with the RCMP.

20 SIRC was advised during a briefing that information-sharing, and in general maintaining strict control over coordination with law enforcement, will be more challenging when decisions have to be made quickly.

21 The Supreme Court in its McNeil decision (2009) rejected the notion that "...all state authorities constitute a single indivisible Crown entity for the purposes of disclosure." Although positive from CSIS's point of view, the court in that decision also indicated that other government bodies, including CSIS, may, depending on the circumstances, be considered "other investigating state authorities". Being found an "other investigating state authority" would carry with it the same disclosure obligations as the police.

ATIP version
dated: MAR 2 0 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

provided more information to the RCMP. The judge concluded that it cannot be said "that CSIS took an active role in the police investigation. Were my factual conclusions otherwise...I would have no hesitation in concluding that CSIS was an 'other investigating state authority'"[22], meaning that such a determination will be decided on a case-by-case basis and will depend on the particulars of the case.

Going forward, this ruling provided important guidance with respect to how CSIS and the RCMP should conduct themselves in order to mitigate as much as possible the risks of full disclosure, both to the Service and to the police investigation. In operational terms, what the ruling means, at a minimum, is that CSIS and the RCMP must take steps to maintain the "independent pursuit of their separate mandates". The significance of being considered an other investigating state authority cannot be overstated, because such a determination would subject CSIS to the same heavy disclosure obligations as the police. Whether and under what conditions CSIS could be considered an investigating state authority is thus a key question for CSIS in terms of managing - and limiting - the risks associated with disclosure of its intelligence in court proceedings.

As a result, CSIS has taken measures to institutionalize the requirements of "separate and distinct". SIRC learned that CSIS and the RCMP have gone some distance towards discussing and distilling best practices from the Toronto 18 investigation. At the time of writing, the Service is involved in a best practices exercise with the RCMP, the goals of which are to develop a framework for dialogue between CSIS and the RCMP at the strategic and operational levels, and to integrate the concept of the separate and distinct investigations into both agencies' training programs. It is anticipated that this will facilitate and improve the cooperation and disclosure process.[23] SIRC assesses this to be an important exercise that will contribute to the dissemination of the insights of the Toronto 18 case throughout CSIS regions and operational branches, where counter-terrorism cases are managed and decisions made.

CSIS has been emphasizing the importance of training and exercises to reinforce the understanding within the Service and the RCMP of the differences between their respective mandates. The Service is moving away from relying too heavily on policy as a solution to every issue.[24] To that end, the RCMP and CSIS have developed the Joint Operational Workshop, "allowing employees of each organization to share ideas, learn about each other's mandates and expand upon ways in which they could work in a

---

22 R. V. Ahmad et al., Ruling No. 14 (May 8th, 2009) Brampton CRIMJ(F)2025/07 (Ont. S.CJ) at paragraph 12.

23 The outcome of this process may be a document that will be appended to the MOU.

24 SIRC Overview Briefing with Senior Management on the Toronto 18 case, November 19, 2010.

ATIP version
dated: MAR 2 9 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

more cooperative and effective manner".[25] Additionally, the RCMP and CSIS developed the Joint Strategic Workshop for Senior Management, the first of which was held in February 2009. Topics included: information-sharing between organizations; the differences between intelligence and evidence; and a discussion of the lawful authorities of different agencies.

Overall, SIRC finds that CSIS's initial response to the "separate and distinct" ruling has been appropriate and commensurate with the significance of this ruling, which provides important guidance with respect to how the Service can minimize its disclosure obligation and still cooperate successfully with law enforcement in counter terrorism investigations.

4.2 Full, Fair and Frank Disclosure

The second ruling of the Toronto 18 case, delivered in December 2009, focused on the role played by CSIS in the process that led to the granting of the RCMP's first warrant. In brief, information CSIS provided to the RCMP in late 2005 via three advisory letters was incorporated in the latter's affidavit. The issue was whether CSIS was under obligation to make full, fair and frank disclosure when it passed on information for the purpose of assisting the police in obtaining a warrant.[26]

The defense counsel cross-examined CSIS on aspects of the advisory letter process. A CSIS official testified that only information believed to be reliable was included in advisory letters; therefore, CSIS "filtered the information for reliability based on its own intelligence assessment" before it was included in an advisory letter.[27] Although the judge accepted that CSIS meant to convey only reliable information to the RCMP, and

---

25 Between 2007 and 2009, four such workshops were delivered, with a total of 46 candidates.

26 The defense argued that the authorizations should be quashed because CSIS, through the advisory letters, intentionally misled the court, failed to provide full, fair and frank disclosure, and destroyed notes in violation of the *Charter* rights of the accused. R. V. Ahmad et al., R. V. Ahmad et al., Ruling No. 23 (December 2, 2009) Brampton CRIMJ(F)2025/07 (Ont.S.CJ) at paragraphs 24 and 29.

27 R. V. Ahmad et al., Ruling No. 23 (December 2, 2009) Brampton CRIMJ(F)2025/07 (Ont.S.CJ) at paragraph 75.As an aside,though there is an obligation for full, fair and frank disclosure, CSIS has to be careful not to disclose too much information, lest it be considered part of the Crown. As a result, when the Service was approached by the affiant, who wished to independently verify the information provided by the Service in its Advisory Letters, CSIS did not respond to the RCMP request that CSIS might be seen as "part of the Crown investigation" if the Service opened up its investigation to the RCMP. Briefing Note re. Garofoli Decision in OSAGE Prosecution at Brampton, Ontario (December 3, 2009)

ATIP version
MAR 2 0 2019
dated:

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

thus did not intend to mislead the RCMP or the Court, he concluded that the advisory letters "were not written in compliance with the rigors of full, fair and frank disclosure" since compliance with this principle would have required CSIS to undertake complete disclosure of information relating to the matter. He concluded that CSIS "should either have fully disclosed that it was simply providing its intelligence opinion and was not including all information bearing on the matters discussed, or it should have made full, fair and frank disclosure."[28]

The Service promptly responded to the issue of full, fair and frank disclosure. In early January 2010, as noted, the DDO issued a *Directive on Disclosure of Service Information to the RCMP, Police and Other Law Enforcement Agencies* to offer some adjustments to current practices. In this Directive, employees are told that once a decision to share specific operational information is taken, "operational branches will conduct a thorough facting exercise" to ensure that the information provided is accurate and balanced, "accounting for any information which would tend to contradict the Service's suspicions or conclusions [...] In every instance, particular attention should be paid to providing any potentially exculpatory information to the RCMP and, by extension, the court." The DDO further specifies that opinions or assessments based on facts "should be clearly identified as such" and that the entire process is to be verified by a senior operational manager, who reviews the draft RCMP document to ensure the information contained therein is consistent with CSIS's original operational reporting.

SIRC is hopeful that the process and measures outlined in the DDO Directive on disclosure of CSIS information will help ensure that, in future criminal prosecutions, information provided by CSIS to law enforcement complies with the requirement to make full, fair and frank disclosure of information relevant to an RCMP warrant application or it should be specified that the Service is simply providing its intelligence opinion.

---

28 R. V. Ahmad et al., Ruling No. 23 (December 2, 2009) Brampton CRIMJ(F)2025/07 (Ont.S.CJ) at paragraph 77. In the end, Justice Dawson nonetheless concluded that CSIS was not involved in an "intentional effort to mislead the RCMP or the authorizing judge" and that "CSIS had a basis to believe that the omitted information was unreliable."

ATIP version
MAR 2 0 2019
dated:

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

5 ISSUES FOR CONSIDERATION

The approach used during the Toronto 18 fared well during prosecution, and CSIS's response to issues identified by the court was appropriate. In recognition of the fact that discussions with respect to "intelligence to evidence" are ongoing and will likely continue for some time, SIRC wishes to flag three areas that CSIS may want to examine more closely as it considers how to move forward.

5.1 Disclosure and Advisory Letters

Of equal importance to the guidance provided by the court on the preparation of CSIS advisory letters, are the issues arising from the mechanism used to disclose information to the RCMP. CSIS shares information with the RCMP via a two-letter system. The first, a disclosure letter, is to be treated as a tip or an investigative lead to initiate or advance a criminal investigation; it is not to be used by police to obtain warrants. The second, an advisory letter, is the formal means by which CSIS authorizes law enforcement to use its information in applications to the court. This letter is carefully prepared and well-vetted, and information contained therein can be used, subject to any attached caveats, for the purpose of obtaining warrants.[29]

The advisory letter is also subject to a more rigorous review process: once an advisory letter is drafted, it goes through multiple stages of review by various levels of management.[30]

Past SIRC reviews have highlighted issues related to the two-letter approach. In 2007, for example, Toronto Region advised that it had undertaken the general philosophical approach of providing the RCMP "with actionable intelligence, of high value, on an infrequent but necessary basis, through the advisory letter process rather than providing unsupported investigative leads through the traditional disclosure letter process." The Region added that, generally, it found disclosure letters "to be somewhat impractical" and "not always the most efficient and effective medium for our law enforcement partners."[31]

---

29 As conceived, an advisory letter should normally be preceded by a disclosure letter, and should only be provided upon a formal request by law enforcement.

30 R. V. Ahmad et al., Ruling No. 23 (December 2, 2009) Brampton CRIMJ(F)2025/07 (Ont.S.CJ) at paragraph 73.

31 SIRC Study 2006-06, CSIS ER&L memo to SIRC (April 12, 2007), question 7.

ATIP version
MAR 2 0 2019
dated:

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Similarly, the RCMP reportedly does not like the two-letter system because it feels it gives "the Service a false sense of security over what information they can protect" and "forces the RCMP to come back to the Service and report to [CSIS] on how they want to use [CSIS's] information before they do."[32]

In fact, Toronto Region's opinions were echoed in a joint CSIS-RCMP report produced in the summer of 2007, which laid a framework for improved collaboration between the two agencies. The report noted that the categorization of advisory and disclosure letters appeared "out of step with current legal disclosure requirements in the criminal justice system," and recommended the adoption of a one-letter system to facilitate the use of security intelligence in an investigative or judicial process. The report offered further guidance, namely that

- both CSIS and the RCMP should draw on their respective legal counsel in drafting these letters;
- the letters should be concise, focusing on elements of a criminal offense in order to expedite the RCMP's engagement in the case, while protecting CSIS sources and methods;
- the letters should clearly indicate how the information is to be used, and contain necessary restrictions regarding who should have access to the information and tailored caveats concerning the use of intelligence for prosecution and disclosure purposes; and
- centralization of this process at the HQ level would help to achieve consistency in disclosure practices and controlled use of information.[33]

The recommendation to adopt a one-letter system was not acted upon despite strong arguments in favor of the one-letter model, which are alluded to above. Some individuals within the Service expressed concern that a single letter system would diminish CSIS's control over its information by giving law enforcement too much leeway to use CSIS information.[34] Yet, it goes without saying that the current procedure that allows CSIS to review and authorize the use of Service information contained in advisory letters prior to its use in RCMP affidavits / court documents must be upheld.

From SIRC's perspective, the most compelling is the Service's providing the RCMP, to the extent possible, with "useful and useable" information. This practice would be better supported through the one-letter system, since there would be fewer limitations (caveats notwithstanding) on how CSIS information could be used by law enforcement.

---

32 DDO Operations Conference, January 2010.

33 CSIS and the RCMP, *Intelligence to Evidence: A Framework for Enhanced Cooperation* (July 2007), pp.13-14.

34 SIRC Briefing on Disclosure and Cooperation with the RCMP, December 22, 2010.

ATIP version
MAR 2 3 2019
dated:

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

The DDO Directive requires CSIS employees to develop an operational and disclosure strategy at the outset of any disclosure, meaning that similar considerations already guide the Service in sharing any information with the RCMP. In the end, any information CSIS shares with the RCMP may be subject to public disclosure; it therefore stands to reason that CSIS should have in place a process designed to ensure that every disclosure to law enforcement goes through a rigorous legal review.

In order to improve the quality and value of the information CSIS provides to its law enforcement partners, and to bring consistency to the way in which CSIS discloses information to law enforcement, SIRC recommends that CSIS adopt a one-letter disclosure model that incorporates the standards of rigorous legal review currently set for advisory letters.

5.2 Verbal Exchanges

The importance of cooperation, early and often, with the RCMP was consistently reinforced to SIRC through briefings and document review. Cooperation entails exchanges at multiple levels, both formal and informal, inside and outside the context of an active investigation. In fact, the judge in the Toronto 18 prosecutions and former Supreme Court Justice Major have both expressed general satisfaction at the level of cooperation between the two agencies.

The DDO Directive of 2010 mentioned earlier establishes the framework governing formal written disclosures of information through the disclosure and advisory letter process; similarly, verbal disclosures need to be recorded and tracked in much the same way. The Directive contains a statement with respect to "Meetings," to the effect that "Headquarters and Regional branch managers are encouraged to continue dialogue with their RCMP counterparts in ongoing efforts to cooperate and de-conflict investigations. There should be a record of these exchanges including, for example, the date, the participants, the topic, the conclusion and the respective rationale for any decisions made."[35]

In the Toronto 18 "separate and distinct" ruling, the judge made reference to the frequent exchanges between senior regional CSIS and RCMP officials. Although the judge accepted that these exchanges were at a strategic level[36], and thus did not represent verbal disclosures per se, SIRC nevertheless examined the records of these exchanges to gain a better understanding of the level of coordination and contact that

---

35 "DDO Directive on Disclosure of Service Information to the RCMP, Police and Other Law Enforcement Agencies", January 2010.

36 R. V. Ahmad et al., Ruling No. 14 (May 8th, 2009) Brampton CRIMJ(F)2025/07 (Ont. S.CJ) at paragraph 41.

ATIP version
MAR 2 2019
dated:

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

took place. Upon review, although there are records of JMT meetings and management level exchanges between senior RCMP and CSIS officials at the Headquarters level during the Toronto 18 investigation, it appears that there is a gap in the Service's records of exchanges of the type that were referenced by the judge in the Toronto 18 proceedings - the daily operational and strategic exchanges.

The DDO Directive is recent and so cannot be applied as the standard against which to judge the Toronto 18 investigation. Still, **SIRC considers it important that CSIS keep proper records of verbal exchanges, consistent with recent jurisprudence on the subject of retention, as well as the Service's own approach to retention since the precedent-setting Supreme Court decision in 2008 in *Charkaoui v Canada* that imposed on CSIS a general obligation to retain operational notes**. This is all the more important given that, as Justice Major points out, "the presence of the police imports the full menu of constitutional protections, including rights to disclosure of information, that are afforded persons who are the subject of criminal investigations."[37] In practice, this could mean that exchanges that take place between the RCMP and CSIS at whatever level may be subject to a disclosure obligation pursuant to s. 7 of the *Charter* if those exchanges pertain to an investigation that leads to a prosecution.

5.3 Warrants

The final issue for consideration relates to the use of information obtained from CSIS warrants in criminal proceedings. In the course of the Toronto 18 prosecutions, the Crown chose to excise information from the CSIS advisory letters found in RCMP affidavits . CSIS obtained some of the information it included in the advisory letters through communications intercepts; that information subsequently formed part of the information used by the RCMP to obtain its own warrant, which raised the issue of whether the CSIS intercepts were properly authorized.[38] To avoid the possibility of the judge having to undertake a thorough review of the relevant CSIS warrants, and to avoid providing the accused with further disclosure of information concerning CSIS wiretaps, the Crown decided not to rely on any of the CSIS wiretaps to support the RCMP warrant authorization.[39]

---

37 Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, "Volume Three, The Relationship between Intelligence and Evidence and the Challenges of Terrorism Prosecutions", 2010, p. 25. Although Major is referring in particular to JMT meetings, this same general principle should extend to all meetings involving the police.

38 Justice Dawson points out that, if they were not, the resulting information would have been obtained in violation of s. 8 of the *Charter*, and would therefore have to be excised from the RCMP warrant applications.

39 R. V. Ahmad et al., Ruling No. 23 (December 2, 2009) Brampton CRIMJ(F)2025/07 (Ont.S.CJ) at paragraphs 84-86.

ATIP version
MAR 2 0 2019
dated:

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

SIRC is aware that, in 2005, CSIS undertook a comprehensive re-evaluation of its warrant application process to inject greater "efficiency, discipline and accountability," and to ensure that CSIS meets its obligation to provide full, fair and accurate disclosure of all material facts.[41] In a recent briefing, CSIS senior management reiterated that this obligation is impressed upon CSIS affiants when preparing affidavits for the Federal Court.[42] **Because the information that CSIS provides to other government departments and agencies is increasingly before the courts as part of criminal prosecutions and other court proceedings, SIRC believes the obligation to provide full, fair and frank disclosure of all material facts should be well understood by all CSIS employees.**

41 Letter from CSIS Director to the Chief Justice of the Federal Court, July 22, 2005.

42 SIRC Overview Briefing with Senior Management on the Toronto 18 case, November 19, 2010.

ATIP version
dated: MAR 2 0 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

6 CONCLUSION

The issue of "intelligence to evidence" is complex and covers a lot of ground, not all of which could be addressed in this review. One of the most pressing issues now and for the foreseeable future concerns the retention of information following the Supreme Court's precedent-setting *Charkaoui II* decision in 2008 that found that the Service breached its duties under section 12 of the *CSIS Act* when it destroyed the operational notes of interviews.[43] The issue of retention is tied to that of "full, fair and frank disclosure," since CSIS now has to retain, in order to make available to the courts if requested, original documents used to produce CSIS reports and assessments.

Across government, discussions are taking place on a range of issues that bear on the question of how to manage the risks to all parties associated with using intelligence as evidence. To that end, in its December 2010 *Response to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182*, the Government committed to undertake initiatives to "improve the relationship between intelligence and evidence in criminal proceedings".

As SIRC was told at multiple briefings, issues connected to using security intelligence in criminal proceedings will continue to evolve as CSIS and law enforcement gain more experience in working cooperatively on counter terrorism investigations and as more court decisions provide additional nuance to this area of the law. Nevertheless, the Toronto 18 investigation and the rulings that flowed from the prosecutorial process were significant for a number of reasons. Though not the first, the Toronto 18 represents the largest group of successful prosecutions to date under the *Anti-terrorism Act*. It is thus a good test, both of the legislation and the ability of the Service and the RCMP to operate in this new environment.

SIRC's conclusion is that CSIS responded appropriately to the challenge of full, fair and frank disclosure and has taken steps to understand and institutionalize the requirements of separate and distinct investigations. That said, the Service's approach to this challenge will continue to evolve as it receives guidance, both from the courts and government. As part of its ongoing responsibilities, SIRC will continue to examine the Service's cooperation with the RCMP, one of its most important domestic partners.

---

[43] CSIS responded quickly and developed new guidelines dictating the retention of virtually all information, in the process completely departing from past information retention practices. This approach is fraught with multiple challenges, not the least of which is technological. The Service is now working to develop a more nuanced, sustainable approach. SIRC Briefing on Long Term Retention, January 12, 2011.

ATIP version
MAR 2 0 2019
dated: