Federal Court Cour fédérale

**Date: 20161004**

**Docket:** [redacted]

**Citation: 2016 FC 1105**

**Ottawa, Ontario, October 4, 2016**

**PRESENT: The Honourable Mr. Justice S. Noël**

**BETWEEN:**

**IN THE MATTER OF AN APPLICATION BY [redacted] FOR WARRANTS PURSUANT TO SECTIONS 12 AND 21 OF THE *CANADIAN SECURITY INTELLIGENCE ACT*, R.S.C. 1985, C. C-23 AND IN THE PRESENCE OF THE ATTORNEY GENERAL AND AMICI**

**AND IN THE MATTER OF [redacted] THREAT-RELATED ACTIVITIES**

**[redacted] JUDGMENT AND REASONS**

## TABLE OF CONTENTS

## I. Introduction

### A. *Overview*

[1] In this application for warrants presented by the Canadian Security Intelligence Service [the "CSIS", also referred to as the "Service"] before a designated judge of the Federal Court pursuant to sections 12(1) and 21 of the *Canadian Security Intelligence Service Act*, RSC 1985, c C-23 [the "*CSIS Act*"] , the CSIS, aside from seeking specific warrants, also asks this Court to amend some of the conditions of the draft warrant templates [further referred to as "warrant templates"]. This request stems from three developments: the Federal Court of Appeal's decision in *X (Re)*, 2014 FCA 249, the coming into force of *An Act to amend the Canadian Security Intelligence Service Act and other Acts*, and an ongoing discussion between the CSIS and the Court regarding the need to protect third-party information collected through the operation of warrants notably in file [redacted] Following the publication of the Security Intelligence

Review Committee's 2014-2015 annual report ["the SIRC Report"] in late January 2016, new evidence was filed concerning a CSIS program of collection and retention of information. The Court had never before been fully informed of the existence of the program. The Court, during the hearings, learned that the program had been existence since 2006 yet it had never heard nor seen any evidence on the matter prior to the recent hearings. As I will detail later, suffice to note for now that for the CSIS, "associated data" is a specific type of metadata obtained from service providers. Although these reasons are based on the CSIS's definition of associated data, I feel it necessary to further adapt the term to the specific legal and judicial context at play here (see paragraph 31 and following). (Canada, Security Intelligence Review Committee, *SIRC Annual Report 2014-2015: Broader Horizons: Preparing the Groundwork for Change in Security Intelligence Review*, (Ottawa: Public Works and Government Services Canada, 2015).) (Canada, Bill C-44, *An Act to amend the Canadian Security Intelligence Service Act and other Acts*, 2nd Sess, 41st Parl, 2015.)

[2] Following the SIRC's Report, this Court convened an *en banc* hearing where proposed amendments to the warrant conditions templates and the collection and retention program were discussed. An *en banc* hearing is one where all available designated judges attend, may participate, and hear the evidence tendered. This format is helpful as it allows the presentation of evidence pertinent to future warrants applications and helps avoid repetition. Designated judges can also benefit from each other's perspectives. In this *en banc* hearing, the Court heard evidence relevant to warrant applications over a four-day period.

[3] I have been mandated by the Chief Justice's to deal with all matters related to the issues raised in this application, meaning that, although all designated judges attended the hearings, I am the sole decision maker in this application; I write these reasons with full judicial independence. I have attached, at "Appendices B" of these reasons, not only a bibliography of the documents submitted by the sets counsel involved, but also source documents that I consider essential readings for this file. The volume of the works consulted is substantial, but necessary to obtain a proper and broad understanding of the issues before the Court today. Sets of counsel referred to the McDonald Commission's reports and to excerpts from Hansard and from a committee of the House of Commons; I will discuss, cite, and contextualize these documents later. After having carefully read the submissions and the books of authorities submitted, in order to properly fulfil my judicial role, I thought it necessary to consult the details of the primary sources referred to by counsel in order to ascertain the legislator's intent (see, for example, paragraph 62 of these reasons). In addition, given that the *CSIS Act* contained a review clause, I took notice of the report on the statutory review and of the corresponding response.

[4] Due to the important issues raised by the proposed amendments to the warrant conditions and by the collection and retention program, I appointed two *amici curiae* (Mr. Gordon Cameron and Mr. François Dadour) [the"*amici*"] who participated at the *en banc* hearings, received all documentation, cross-examined witnesses, and filed submissions. I have benefited from written submissions from the Attorney General, counsel for the CSIS, and from the appointed *amici*. I ultimately issued the warrants but only accepted the conditions as they read prior to the proposed amendments. By doing so, I relied on conditions developed and reviewed over several years and took under reserve the proposed amendments to the warrant templates. Among other concerns, I

also reserved accepting the amendments related to the issue of information collected and retained through the operation of a warrant along with the other proposed amendments.

[5] The text, context and purpose of the *CSIS Act* surrounding the enactment of section 12(1) of the *CSIS Act*, formerly section 12 prior to 2015, establishes that strictly limiting the CSIS's mandate was inherent to the legislator's intent. As such, the functions of both collection and retention of information must be performed only to the extent that is strictly necessary. On the other hand, the Court finds that strictly limiting the analysis function of the CSIS is unwarranted and runs counter to the legislative intent identified and to common sense. As long as the information analysed is collected and retained because it is threat related pursuant to section 2 of the Act, no limit must be imposed on the extent of the analysis that may be performed by the CSIS.

[6] The information collected and retained pursuant to sections 12(1) and 21 of the *CSIS Act* must be information related to a threat to the security of Canada, which focuses on information that relates to the target of the warrant. Section 21 is not a scheme operating independently from the primary mandate and functions established at section 12(1). Threats to the security of Canada are circumscribed at section 2 as activities involving the target as determined through investigation. Presently, in order to retain the information collected pursuant to the warrant conditions, the CSIS must assess this information within the one-year time period stipulated in paragraph 21(5)(b) to determine whether it is indeed linked to the identified threat or may be of some use to a prosecution, national defense, or international affairs. Specifically, due to the

illegality identified, information unrelated to the threat and linked to third parties must not be retained as it does not fall within the ambit of the warrants issued by the Court.

[7] In addition, the CSIS has breached its duty of candour towards the Court by failing to inform it clearly and transparently of its retention program, more specifically in regard to associated data collected and retained through the operation of warrants. Each of these conclusions will be detailed over the course of these reasons, which also include findings as to the proposed amendments to the warrants templates.

[8] To approach this complex decision, I will now describe the general structure of the following reasons. First, I will provide an overview of the relevant facts, terminology, legislation, and legislative history. Second, I will expose the submissions presented by the Attorney General, counsel for the CSIS, and the *amici*. Third, I will identify the legal issues raised. Fourth, I will perform an analysis containing several chapters. The first chapter will discuss the duty of candour. The second chapter, the longest, will elaborate as to why the primary function of the CSIS to investigate threats is limited “to the extent that it is strictly necessary” (sections 12(1), 2 and 21). Having done so, the third chapter will explore the practical effects of my findings on the Service, notably in regard to the amendments sought to the warrants templates. Finally, I will conclude briefly and add closing comments. It will be suggested that the legislation of 1984 calls for a review in order to answer to the needs of the present and or unforeseen times ahead with an adaptation to new technologies at play. There is a need to rediscuss the benefits of insuring a better national security but with the least intrusion on privacy. A proper balance of these new technologies must be performed.

B. *Factual Context*

[9] Designated judges have always kept a close eye on the wording of warrants. They continuously try to ensure that the powers granted by the warrants are clearly defined, that the information collected and the means taken are proportionate to the threat, and that such information relates only to the target of the warrant and not to innocent third parties unassociated to the threat factually described in each warrant application.

[10] Warrants are live documents that require continual review by designated judges with input from counsel for the CSIS and appointed *amici* (where thought to be necessary). Amendments are periodically brought to the warrant conditions templates in order to faithfully reflect the powers intended to be granted and their limits. The templates must be adapted to the evolution of technology, of investigative methods, of programs and means of communications, of case law, and of new laws or amendments to the *CSIS Act*. The present reasons are an example of such a periodic examination of the warrant conditions templates.

[11] In 2005, a CSIS task force recommended the Service retain all data collected from investigations and warrants in order to exploit that information in ongoing and future investigations through a technological program. As a result, the Operational Data Analysis Centre [the "ODAC"] was created and became operational in April 2006.

[12] The CSIS originally intended to present the ODAC program to the Court and to seek its comments, along with its new position on retention of data unrelated to identify threats collected

through the operation of warrants (see paragraph 31). It presented the program to the responsible Minister but not to the Court. It was only in December 2011, at an *en banc* hearing called to deal with the proposed amendments to the warrants templates in response to *Charkaoui v Canada (Citizenship and Immigration)*, [2008] 2 SCR 326, 2008 SCC 38, [further referred to as "*Charkaoui II*" given that *Charkaoui v Canada (Citizenship and Immigration)*, [2007] 1 SCR 350, 2007 SCC 9, "*Charkaoui I*" was rendered prior] that an indirect allusion was made to the program. Counsel for the CSIS alluded to the program but did not mention its name or what it consisted of. The allusion came about as a result of my invitation to counsel for the CSIS to add anything as a final comment. Counsel for CSIS said: "[…] these are other minor changes to the conditions that we think go to clarity […] we also looked at trying to better the language […] not change to better the language." More on this exchange later. (See transcript of file [redacted] dated [redacted] at 83-85).

[13] These "minor changes" in fact distinguished "associated data" from "content". Information deemed "content", according to relevant warrant conditions, is to be destroyed. By inserting the word "content" into the condition, the CSIS effectively rendered it silent on "associated data". This change was not performed in response to *Charkaoui II*, but rather for operational reasons, as the historical record of the ODAC and use of associated data shows.

[14] Following this seemingly innocuous "minor change", the CSIS later adopted the position that it had explained "clearly and transparently" the retention of associated data to the Court. However, the SIRC, which studied CSIS's use of metadata, concluded in its 2014-2015 annual report that the CSIS should have been more explicit with the Court.

[15] Following two (2) days of *en banc* hearings in March 2016, in a letter dated April 29, 2016 the Attorney General and the counsel for the CSIS acknowledged that the Court was not: "[…] fully advised of the Service's practices with respect to retention of associated data" and that "[i]t was deeply regrettable that this was only done recently".

[16] In mid-2015, in the application for warrants indexed as [redacted] which I was assigned to, the CSIS proposed a series of amendments to the warrant conditions templates. The changes proposed in that application were presented as consequential to the decision *X (Re)*, 2014 FCA 249, in turn giving effect to the decision *X (Re)*, 2013 FC 1275, and as a result of the coming into force of Bill C-44, also known as *An Act to amend the Canadian Security Intelligence Service Act and other Acts*. Due to the importance of the changes sought, an *amicus curiae*, Mr. Gordon Cameron, was appointed.

[17] In application [redacted] the Court considered amendments proposed by the CSIS which aimed to ensure compliance with new legislation, mainly regarding the sharing of information with other international intelligence agencies. This issue was resolved with input from both counsel for the CSIS and the *amicus*: amendments to the warrants templates were accepted to impose on the CSIS an obligation to consider potential harm to the person concerned as a result of the shared information. I raised other issues in that same application, notably the CSIS's undertaking [redacted] and the issue of collecting and retaining non-threat and third-party related information. The overarching purpose of these discussions was to debate the possibility of an assessment period for retention shorter than [redacted] On six occasions, a hearing was held to discuss all of these issues; I will

comment further on this topic later. The application for warrants in file [redacted] was granted with some amendments concerning the sharing of information.

[18] As for the other matters, counsel for the CSIS requested time to review them in light of the Service's relevant operational needs. At the request of counsel for the CSIS, the period granted to answer the Court's concerns was extended twice from the initial deadline of September 2015: first to October, and ultimately to December 2015. It was only on December 8, 2015 that a letter from counsel for the CSIS to the Court broached the topic of the definition of the term "destroyed" and the topic of the assessment period required by the CSIS to decide what information may be retained in conformity with the warrant conditions. It contained numerous amendments to the warrant templates. At no time during the many hearings, or in any correspondence thereafter, was it mentioned that the CSIS was retaining data concerning third parties unrelated to threats as defined in the conditions required for a warrant to be issued although such retention was the crux of the Court's concern about non-threat, third-party information. All of the further amendments sought in [redacted] were to be dealt with in a later application for warrants.

[19] Some of those amendments were assessed with relative ease: in a direction issued January 11, 2016, the Court accepted the amendment concerning the word "obtention" and a second amendment suggesting a shorter retention period for certain types of warrants [redacted] rather than [redacted] for [redacted] warrants). That same direction scheduled another *en banc* hearing in order to address the other substantial changes sought which required *viva voce* evidence. This *en banc* hearing, which became file [redacted] the present proceeding,

was scheduled to be held from February 25 to February 26, 2016. Two further days of hearings were held on March 31 and April 1, 2016.

[20] In this application, the CSIS seeks amendments to the warrants templates as follows:

> a) A provision allowing the Service to retain [redacted]
>
> b) A new condition allowing the Service to retain [redacted]
>
> c) A new condition specifically and explicitly governing any [redacted]
>
> d) ) A new condition explicitly stating that information destroyed pursuant to a warrant condition [redacted]
>
> e) New wording describing the persons responsible to determine whether information, communication, or oral communications collected should be retained, i.e. replacing all references to a "Regional Director General or his designate"; and
>
> f) A series of stylistic or minor changes."
>
> (See Written Submissions of the Applicant at para 12.)

In regard to condition (e), as a result of the *en banc* hearing, the CSIS now proposes that the wording should read "Regional Director" for some decisions and "Service employees" for others.

[21] The public *2014-2015 SIRC Annual Report* was tabled on January 28, 2016 in the House of Commons and made public the CSIS's retention of collected information through the operation of warrants. This was the first time I understood that the Service was indefinitely retaining third party information as a result of the operation of warrants.

[22] The day following my reading of the SIRC Report, as part of the [redacted] application (this file), I issued a direction to the CSIS communicating that the upcoming *en banc* of late February 2016 would need to address this new matter and that an affidavit should be filed that would "[…] explain in chronological order the various interpretations adopted by CSIS with respect to metadata use and retention practices by referring to the applicable warrant language, the date of proposed language changes with the exact reference to the application for warrants where counsel brought to the attention to the Court the nature of the use of metadata, such use and retention being in the Service's view in compliance with the exception to the warrant conditions". I directed that the affiant be available for examination on the two (2) days already scheduled and that *amici* would be appointed to assist the Court; Mr. Gordon Cameron and Mr. François Dadour were appointed.

[23] On that same day, the Federal Court's designated proceedings registry received a letter from the Assistant Deputy Attorney General (Litigation) addressed to the Chief Justice of the Federal Court. The letter stated that, at the *en banc* hearing of December 16, 2011 the CSIS had "clearly communicated […] the retention program of associated data […]". The letter further indicated that "[…] to ensure that there can be no confusion on this issue going forward […]" counsel had already made changes in the affidavits in support of two warrant applications [redacted] at paragraph 91 and [redacted] at paragraph 71) by adding the following information and bringing it to the attention of the presiding judge:

> "When a communication is intercepted, the Service obtains the content of the communication but also its associated data. Data associated to any communication collected by the Service is retained except in the following two situations:
>
> a) Data associated to solicitor-client communications is destroyed at the same time as the

> content of the communication in application of the solicitor-client communications condition found in the warrants; and
>
> b) Data associated to certain voice communications intercepted under the authority of the [redacted] warrant is destroyed at the same time as the content of the communication in applications of the conditions found in the warrant."

Contrary to what was said in that letter, such information was not addressed by counsel for the CSIS at the 2015 hearings. Therefore, what the Assistant Deputy Attorney General (Litigation) wrote in his letter was not factual. Counsel for the CSIS, at the first day of the *en banc* hearings said the following:

> "It's unfortunate that at the hearing of August the addition of associated data in the affidavit was not mentioned. Looking back it's definitely something that should have been brought to the attention of the Court to give a bit of context as to why it was added"
>
> (See transcript of *en banc* hearing dated February 25, 2016 at 58.)

As mentioned above and as I will elaborate later, the Attorney General and the CSIS now concede that the retention program of the data collected through the operation of warrants was not clearly communicated.

[24] The Chief Justice, after receiving more information following an exchange of letters with the Assistant Deputy Attorney General (Litigation), called for another *en banc* hearing to address the systemic issues arising from the CSIS's behaviour towards the Court in relation to the retention program of associated data and other related concerns. This *en banc* hearing, where both the Deputy Attorney General and the Director of the CSIS appeared, was held in the

afternoon of June 10, 2016. The following reasons do not deal with the June 10, 2016 hearing but address the various matters raised in file [redacted] (this file) which include issues related to the ODAC program and whether the Court was properly informed of its existence. As said, these reasons also address the amendments sought by the CSIS as a result of the hearings held in file [redacted] which led to the letter of December 8, 2015 referred to above at paragraph 18.

[25] The *en banc* hearings on these matters, which I presided over, were held over four (4) days in February, March and April 2016. Five affidavits were filed and three affiants were examined by counsel for the CSIS, by the *amici*, and by some of the designated judges, including myself. A large number of exhibits were produced. Both the oral and written evidence address the ODAC, the retention of associated data, and the operational explanations supporting the amendments sought to the warrant templates. Written submissions were filed by both sets of counsel and a reply authored by counsel for the Attorney General and the CSIS was received. Having reviewed the factual underpinnings of these reasons, I will now detail certain useful terms and concepts.

C. *Terminology and Useful Concepts*

[26] Before I begin, I want to establish that the vocabulary and definitions I use are useful to establish the scope of these reasons but that they are not meant to be binding in any other circumstances. I am cognizant of the fact the CSIS and other parties use varying definitions and concepts to suit their own needs. First, I will describe the phases of an intelligence investigation. Second, I will delineate the term “associated data” and third, present an outline of the ODAC program as revealed by the evidence.

(1) Phases of an Intelligence Investigation

[27] First, the CSIS, at the initial stage of an investigation, identifies persons of interest (persons, groups, or states) that may, for one reason or another, have come to its attention for possibly being related to a perceived threat. A person may draw the attention of the CSIS through different means, notably from tips, from certain behaviours, or as a by-product of other domestic or international investigations. At this initial step, the CSIS will consult its database and publicly available information in order to assess whether the facts reveal a nexus to a section 2 definition of threats to the security of Canada. At this initial assessment stage, the person investigated is referred to as a "person of interest". The graph below summarizes the three phases and their associated vocabulary.

| | |
|---|---|
| Step 1 | "person of interest" |
| Step 2 | "subject of investigation" |
| Step 3 | "target of investigation" |

[28] Second, pursuant to section 12(1), if the CSIS reasonably suspects that the facts involving or implicating the person of interest relate to activities that may constitute a threat to security in accordance with the definitions of threats found at section 2, then that person becomes a "subject of investigation". Once the person is deemed a "subject of investigation", the CSIS can deploy conventional tools of investigation such as the involvement of a human source, physical surveillance, and any other tool or method normally available to police forces or intelligence services. This stage of investigation does not permit the use of intrusive investigative methods for which a warrant is required.

[29] Third, if the CSIS believes, on reasonable grounds, that a warrant is required to investigate the threat, then the Service may approach the Minister of Public Safety and Emergency Preparedness to obtain his approval to proceed with an application for a warrant in accordance with sections 21(1) and 21(2) of the Act. If the CSIS proceeds with such an application and is successful, a warrant is issued and the person designated in the application becomes a "target of investigation". The graph below summarizes my explanations; it is not meant to be exhaustive.

| **Step** | **Standard** | **Nomenclature** | **Scope of means of investigation** |
|---|---|---|---|
| Step 1 | The CSIS becomes aware that the person may be of interest. | "Person of interest" | Publicly available information and searches in databases |
| Step 2 | The CSIS has reasonable grounds to suspect that the person may be a threat. | "Subject of investigation" (sections 12(1) and 2) | Conventional investigative means |
| Step 3 | The CSIS must reasonably believe that intrusive measures are necessary to investigate the threat, and the warrant is granted. | "Target of investigation" (sections 12(1), (2) and 21) | All conventional and intrusive investigative means |

[30] These descriptions of the phases of an investigation pursuant to the *CSIS Act* are my own; the CSIS may use different vocabulary or concepts for its own purposes. The purpose of explaining the phases is to show that the present reasons deal with the information collected by the operation of warrants issued by the Federal Court. Specifically, these reasons do not address other forms of collection as no evidence was presented to that effect. Still, the present reasons may establish general principles for future purposes. Having said that, associated data is an essential component of these reasons and I will frame the concept as the CSIS describes it and also as the evidence reveals.

(2) What Is Associated Data?

[31] Although the concept of associated data is broad, in fact englobing third-party information and target-threat related information, I am specifically addressing the legality of retaining non-threat information and third-party information. Third-party information, meaning information unrelated to the threat, is frequently collected through the operation of warrants. The Court is concerned about the retention of such information because it is not target-threat related. Warrant conditions oblige the CSIS to review third-party information it has collected in order to assess whether or not it falls within the conditions' parameters and thus whether or not it can be retained. The term used by the CSIS to describe this specific type of information when obtained from service providers is "associated data". The CSIS described the term as follows in an affidavit, but I note that witnesses sometimes referred to the term more broadly in their testimonies:

> "[I]nformation associated to a communication such as [redacted]
>
> See Supplementary Affidavit of [redacted] filed February 22, 2016 at page 18, footnote 10.) (See transcript dated Thursday March 31, 2016 (Examination of [redacted] at 41-42.) (See transcript dated Thursday March 31, 2016 (cross-examination of [redacted] by Mr. Dadour) at 77-80, 90, 100-103.)

[32] As per either the present conditions 2 or 3 of some of the warrant conditions templates, the CSIS must review the information collected through warrant operations [redacted] to ensure that information involving third parties is indeed threat related. If the information is deemed unrelated to the threat, it must be destroyed. When performing its assessment, the CSIS must believe on reasonable grounds that the information may be either related to the

investigation of a threat, or of assistance to an intelligence investigation or to a prosecution, to national defense, or to international affairs. Such a test gives the CSIS a certain level of discretion. The condition defining these parameters reads as follows:

> "Subject to condition 1, any record, document or thing obtained pursuant to this warrant that is not destined to or does not originate from [the target] […] shall be reviewed by a Regional Director General or his designate and, unless he has reasonable grounds to believe the record, document or thing may (a) assist in the investigation of a threat to the security of Canada; (b) be used in the investigation or prosecution of an alleged contravention of any law of Canada; or (c) relate to the international affairs or defence of Canada, any copy of the record, document or thing shall be destroyed within a period of [redacted] following its obtention."
>
> (See condition 2 or 3 of certain warrant templates. The above relates to a [redacted] while the others are written in such a way as to adapt to the specifics of the particular warrant template. They all contain the same requirement for assessment purposes.)

[33] Over the course of these proceedings, it became clear, through submissions and witnesses, that the definition of associated data for the Court consists of data collected through the operation of the warrants from which the content was assessed as unrelated to threats and of no use to an investigation, prosecution, national defense, or international affairs. (See affidavit of [redacted] received March 24, 2016 at paras 47, 56-67, 90-92.)

[34] The following graph illustrates where associated data fits within a more general framework of the CSIS's operations; I am aware that I am slightly diverging from the CSIS's definition:

| | |
|---|---|
| Step 1: information (content + metadata) is collected | (go to step 2) |

| | |
|---|---|
| Step 2: information is assessed by the CSIS | - If the content is threat related, both content and metadata are retained;<br><br>OR<br><br>- If the content is not threat related, content is destroyed but metadata is retained (go to step 3). |
| Step 3: create and retain "associated data" | - Metadata originating from content unrelated to the threat, for which the content has been destroyed, is called "associated data".<br><br>- The CSIS retains all associated data it has collected for an indefinite period of time. |

[35] As the evidence before the Court now reveals, associated data is retained and inserted into the ODAC program for future investigative purposes. The CSIS has been retaining associated data indefinitely since 2006.

[36] Having established the phases of investigations and defined associated data for the purposes of these reasons, I now turn to describing the ODAC program itself.

(3) Operational Capacities of the CSIS in Relation to Data Exploitation

[37] In the early 2000's, the CSIS considered that the information it collected through investigations was underutilised as it was not processed through modern analytical techniques. In April 2006, the CSIS launched the ODAC. The ODAC was designed to be "a centre for excellence for the exploitation and analysis" of a number of databases. It took approximately [redacted] for the centre to become fully operational. The ODAC assumes numerous tasks: it exploits data banks in order to provide: [redacted]

[redacted] See Executive Summary of the August 10, 2010 *Operational Data Analysis Centre Privacy Impact Assessment*, performed by [redacted] (consultant) and finalized by the ATIP branch of the Canadian Security Intelligence Service. Document located in the book "Documents for Amici" as a supplement to the Affidavit of [redacted] (affirmed April 21, 2016), in file [redacted] at Tab 8.)

[38] The ODAC, up to late 2010, was hosted within the [redacted] which itself renders multi-faceted and specialized support to the CSIS's operations. The ODAC [redacted]

[39] More specifically, the ODAC processes information held by the CSIS through:

> "[…] the authority of a warrant or an approved investigation. As of January 2010 […], the ODAC data holdings consisted of [redacted]
>
> (See letter dated November 8, 2012 to the Office of the Privacy Commissioner, signed by [redacted] Coordinator - Access to Information and Privacy, at p 4. Document located in the book "Documents for Amici" as a supplement to the Affidavit of

[redacted] (affirmed April 21, 2016), in file [redacted] at Tab 10.)

[40] The evidence presented during the hearings did not update this information to 2016 except for what follows. Aside from analysing and processing these datasets into investigative information, the ODAC:

> "[…] provides operational support for these investigative activities by developing actionable intelligence [redacted]
>
> (See letter dated November 8, 2012 to the Office of the Privacy Commissioner, signed by [redacted] Coordinator - Access to Information and Privacy, at p 3 and 4. Document located in the book "Documents for Amici" as a supplement to the Affidavit of [redacted] (affirmed April 21, 2016), in file [redacted] at Tab 10.)

[41] [redacted]

[redacted] The present reasons should not give the impression that the Court is well informed of the [redacted] program; only very limited evidence was provided. Given that the program was still called the ODAC at the time of the application, I will use that term and not [redacted]

[42] The ODAC is a powerful program which processes metadata resulting in a product imbued with a degree of insight otherwise impossible to glean from simply looking at granular numbers. The ODAC processes and analyses data such as (but not limited) to: [redacted] The end product is intelligence which reveals specific, intimate details on the life and environment of the persons the CSIS investigates. The program is capable of drawing links between various sources and enormous amounts of data that no human being would be capable of [redacted]

[43] The Data Exploitation Task Force provides more insight into the initial capacities of the ODAC; [redacted] yet the evidence presented to the Court to this effect was very limited.

[redacted]

> (*Data Exploitation Task Force Draft Report (version 1.3)*, dated July 11, 2005 at 10. Found at "Annex B", Tab 4, of the book provided to the Court in response to the letter of March 23, 2016 from the Chief Justice.)

[44] Information collected through the operation of warrants is fed into the ODAC [redacted] the information is assessed within [redacted] by the CSIS; the content is destroyed if it is found to be non-threat related, or unintended for prosecutorial purposes, international affairs, or the defense of Canada. If the information remains unassessed at the end of the [redacted] it must be destroyed as mentioned above. [redacted] the metadata is retained indefinitely even if the underlying content is found to be non-threat related. As we will see later, understanding [redacted] is important when discussing whether or not a [redacted] retention period is necessary and appropriate.

[45] Now that I have broadly described the terminology, underlying concepts, and the ODAC program in general, I will detail the relevant legislation and provide a historical overview of the *CSIS Act*.

D. *Relevant Legislation*

[46] The central focus of my interpretation of section 12(1) will be to ascertain the meaning of the expression: "[…] to the extent that it is strictly necessary" and its implications for the CSIS's functions. The primary functions of CSIS are the collection, retention and analysis of information. These three functions must be assessed in conjunction with the existence of a threat to the security of Canada as defined in section 2 of the *CSIS Act*. I should mention that I will not

analyse the amendments brought to the *CSIS Act* in 2015 except to note that they provide additional functions to the Service such as the abilities to work internationally (section 12(2)) and to take measures to reduce a threat (section 12.1(1)). In addition, I note that the Court no longer adjudicates applications for warrants to obtain information from the Canada Revenue Agency following the enactment of the *Security of Canada Information Sharing Act*, SC 2015 c 20, s 2. The factual underpinnings of this development can be found in the SIRC 2014-2015 Report at pages 27-28. This new piece of legislation expanded and facilitated the sharing of information among certain listed Government of Canada institutions that have jurisdiction or responsibilities concerning national security. In practice, the CSIS no longer needs a warrant to obtain information from the CRA. No submissions were presented by either sets of counsel in regard to these new capacities; they are limited to sections 12(1), 2 and 21 of the Act.

[47] Section 12(1) of the *CSIS Act*, following amendments to the Act in 2015, reads:

| *Canadian Security Intelligence Service Act*, RSC, 1985, c C-23 | *Loi sur le Service canadien du renseignement de sécurité*, LRC, 1985, ch C-23 |
|---|---|
| **Duties and Functions of Service** | **Fonctions du Service** |
| *Collection, analysis and retention* | *Informations et renseignements* |
| 12(1) 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 | 12(1) Le Service recueille, au moyen d'enquêtes ou autrement, dans la mesure strictement nécessaire, et analyse et conserve les informations et renseignements sur les activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada; il en fait rapport au gouvernement du |

| | |
|---|---|
| Government of Canada. | Canada et le conseille à cet égard. |
| [Emphasis added.] | [Je souligne.] |

[48] The wording “threats to the security of Canada” found in section 12(1) is defined in section 2 of the *CSIS Act* to mean:

| | |
|---|---|
| *Canadian Security Intelligence Service Act*, RSC, 1985, c C-23 | *Loi sur le Service canadien du renseignement de sécurité, LRC*, 1985, ch C-23 |
| **Definitions** | **Définitions** |
| 2. In this Act, | 2. Les définitions qui suivent s’appliquent à la présente loi. |
| *threats to the security of Canada* | *menaces envers la sécurité du Canada* |
| means | Constituent des menaces envers la sécurité du Canada les activités suivantes : |
| (a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage | a) l’espionnage ou le sabotage visant le Canada ou préjudiciables à ses intérêts, ainsi que les activités tendant à favoriser ce genre d’espionnage ou de sabotage; |
| (b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person, | b) les activités influencées par l’étranger qui touchent le Canada ou s’y déroulent et sont préjudiciables à ses intérêts, et qui sont d’une nature clandestine ou trompeuse ou comportent des menaces envers quiconque; |
| (c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within | c) les activités qui touchent le Canada ou s’y déroulent et visent à favoriser l’usage de la violence grave ou de menaces de violence contre des personnes ou des biens dans le but d’atteindre un objectif politique, religieux ou idéologique au Canada ou dans |

| | |
|---|---|
| Canada or a foreign state, and | un État étranger; |
| (d) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada, | d) les activités qui, par des actions cachées et illicites, visent à saper le régime de gouvernement constitutionnellement établi au Canada ou dont le but immédiat ou ultime est sa destruction ou son renversement, par la violence. |
| but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (a) to (d). (*menaces envers la sécurité du Canada*) | La présente définition ne vise toutefois pas les activités licites de défense d'une cause, de protestation ou de manifestation d'un désaccord qui n'ont aucun lien avec les activités mentionnées aux alinéas a) à d). (*threats to the security of Canada*) |

[49] Section 21 is also important; it is the procedural section that instructs the CSIS as to how to apply for warrants to the Federal Court if conventional means of investigation are not sufficient to advance the investigation. As section 21 is quite lengthy, it may be found in the "Appendices" section at the end of these reasons. (See Appendices A – Relevant Legislation.)

E. *Historical Overview*

[50] As I will elaborate at paragraphs 117-149 below, the historical record demonstrates that the legislator intended to substantially limit the mandate and functions of the CSIS in regard to section 12(1). The results of multiple factors found in the various sources of legislative intent are highly convergent. All sources, from the McDonald Commission's recommendations, to the Pitfield Report, to the Solicitor General's explanations during the clause by clause review of the

Standing Committee on Justice and Legal Affairs, point to the overarching principle that the mandate and functions of the CSIS should be strictly defined and limited (details below).

[51] Following the establishment of the Royal Commission of Inquiry into Certain Activities of the RCMP in 1977, also known as the McDonald Commission, and the final publication of its recommendations in 1981, the government of the day introduced Bill C-157 in the House of Commons to establish a civilian intelligence security service. Although I chose 1977 as the most relevant start date, it is obviously possible to refer to relevant events and publications dating further back, such as the Royal Commission on Security in 1969 [the "MacKenzie Commission"] and the Kellock-Taschereau Commission in 1946 [the "Gouzenko Affair"]. (Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (Ottawa: Privy Council Office, 1979, 1981). There are several reports and several volumes, see "Appendices B – Bibliography" for details.)

[52] In June 1983, following widespread opposition, Bill C-157 was referred to a special committee of the Senate, which recommended substantial changes to the bill. In November 1983, the Special Committee of the Senate on the Canadian Security Intelligence Service tabled its comprehensive report titled "*Delicate Balance: A Security Intelligence Service in a Democratic Society*" [the "Pitfield Report"]. Bill C-157 was subsequently allowed to die on the order paper and a revamped Bill C-9 was tabled in its stead. (Senate of Canada, Special Committee of the Senate on the Canadian Security Intelligence Service, *Delicate Balance: A Security Intelligence Service in a Democratic Society*, (November 1983) (Chair: P.M. Pitfield).)

[53] Following the Pitfield Report, the government issued a written response where it indicated which recommendations it accepted, rejected, or accepted in part. The response indicated that the Pitfield Report's recommendation to limit the primary function of CSIS by the addition of a test of "necessity" was accepted. As such, clause 14(1) of Bill C-157 was modified and became clause 12(1) in Bill C -9.

| Bill C-157 | Bill C-9 |
|---|---|
| *Functions of Service* | *Duties and Functions of Service* |
| 14(1) The Service shall collect, by investigation or otherwise, 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. | 12(1) 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.<br>[Emphasis added.] |

[54] Bill C-9 was introduced in January 1984 during the second session of the 32nd Parliament. Bill C-9 included virtually all the changes recommended by the Pitfield Report. It was given first reading in January 1984 and referred to the Standing Committee on Justice and Legal Affairs in March. Bill C-9 passed third reading and was given royal assent in June and was proclaimed in force in two parts over July and August 1984.

[55] The *CSIS Act* enacted in 1984 contained a review clause calling for a review of the legislation to be performed five (5) years following the coming into force of the Act. Such a review was completed in 1990 and the government issued a report in reply in 1991. From 1991 until today, the *CSIS Act* has occasionally been amended, notably by the addition and

specification of certain functions in 2015. I will now review the arguments of both the Attorney General and counsel for the CSIS and the *amici*.

## II. Arguments

### A. *Arguments of the Attorney General and Counsel for the CSIS*

[56] Summarily, in regard to the CSIS's duty of candour towards the Court, the Attorney General of Canada and counsel for the CSIS [collectively the "AGC"] suggest that the Court was indeed advised of the retention program, although not as thoroughly as warranted; no evidence of "systemic obfuscation" has been adduced. Regardless, the Service has committed, going forward, to advise the Court of any proposed changes in practice without delay. In regard to the amendments to the warrant conditions proposed by the *amici*, the AGC contends that the *amici*'s suggestions are impractical.

[57] In the next paragraphs, I will detail the more complex arguments the AGC puts forward. I will first summarize the AGC's argument contending that section 12(1) and section 21 are separate schemes operating independently from each other. Later, concerning the legality of the associated data retained, I will detail the AGC's arguments contending that the *amici*'s analysis of privacy interests in relation to section 8 of the *Charter* is flawed, and will elaborate on what the AGC considers justifiable in respect to the retention of such data. Since I am concluding that the CSIS does not have the jurisdiction to retain non-threat information related to third parties, I will not deal with the privacy arguments submitted, apart from making brief comments further below. However, I have included the arguments for the sake of future reference and

completeness. (*Canadian Charter of Rights and Freedoms*, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11.)

(1) Section 12(1) Does Not Apply to Section 21 of the *CSIS Act*

[58] Contrary to the *amici*'s basic position, the AGC asserts that section 12(1) does not apply to section 21 of the *CSIS Act*. In other words, the limits to the Service's actions defined at section 12(1) should not apply to the collection of information following the issuance of a valid warrant. In essence, the AGC suggests that the collection and retention of information operates in two distinct phases with different sets of parameters. In the first phase, the Service is permitted by section 12(1) to obtain basic information. In the second phase, following the granting of a warrant, section 12(1) no longer applies and the collection of information is instead controlled exclusively by the parameters set in section 21.

[59] Limitations found in section 12(1) should only apply to information collected from the application of a warrant issued under section 21 if: (a) section 21 explicitly or implicitly incorporates section 12(1); or (b) if section 12(1) applies to warranted collection under section 21. In the AGC's opinion, both of these options are inapplicable. There is nothing in the wording of section 21 that suggests it was intended to incorporate the restrictions present in section 12(1). Interpreting the matter otherwise risks creating conflicting standards between terms and conditions of warrants and section 12(1).

[60] Alternatively, because section 12(1) and section 21 are found in different parts of the *CSIS Act*, respectively "Duties and Functions of the Service" and "Judicial Control", they should

not be found to apply to one another. Sections 15 and 16 would, for example, be limited by section 12(1) as they are all found in the same part (Part I) of the *CSIS Act*, but section 21 would not be as it is in the next part (Part II). The AGC argues that provisions in one part of a statute may only affect provisions in another part if legislative language supports it. Considering the structure of the scheme, the AGC argues that there is no clear interpretative basis for applying limitations in section 12(1) to some activities of the Service (ex. section 21) but not to others (ex. sections 15 and 16).

[61] Section 21 does not expressly incorporate section 12(1). In addition, section 21(4), which lists matters that must be specified in a warrant, does not reflect any of section 12(1)'s language. Likewise, section 21 does not implicitly incorporate any requirements found in section 12(1). In fact, section 21(3) provides the judge issuing the warrant the power to authorize the interception of "any communication, or to obtain any information, record, document or thing […]".

[62] The AGC responds to the *amici*'s argument that the "strictly necessary" qualifier in section 12(1) applies to both collection and retention by submitting that such an interpretation of the wording runs contrary to the structure of section 12(1) and to the Supreme Court's decision in *Charkaoui II*, above, at para 38. In addition, the AGC asserts that a sentence from a larger explanation given by Minister Kaplan, the Solicitor General at the time the *CSIS Act* was enacted, shows that the expression "to the extent that is strictly necessary" qualifies the collection function but not the retention function:

> "Kaplan: Well I had followed in this amendment the exact recommendation of the Senate Committee. The Senate committee looked at the function of collection as the one that ought to be limited to what is strictly necessary. We do not want them to

> collect any more than is strictly necessary because it is the collection that is the potential violation of people's privacy rights."

As it will be seen later, the AGC, by presenting such a limited sample of a larger discussion, presents Mr. Kaplan as saying something that is contradicted when read in its full context. (House of Commons, *Minutes of Proceedings and Evidence of the Standing Committee on Justice and Legal Affairs*, 32nd Parl, 2nd Sess, No 28 (24 May 1984) at p 28:52 (Chair: Claude-André Lachance).)

[63] The AGC opines that the Supreme Court of Canada, in *R. v Vu*, [2013] 3 SCR 657, 2013 SCC 60, has established that the judiciary effectively balances private and state interests through the issuance of warrants. As such, section 12(1) does not need to apply to section 21 in order for privacy interests to be protected by judges. The only link between section 12(1) and section 21 is that the Service must have initiated an investigation under section 12(1) in order to ascertain the facts required to satisfy the Court that a warrant is required.

(2) Arguments on Privacy Interests

[64] The AGC believes the *amici*'s section 8 analysis in relation to privacy interests and the existence of an expectation of privacy is flawed; they overlook relevant cases and propose an approach unsupported by jurisprudence. The *amici*'s conclusion that the analysis of associated data creates insights into core biographical information of persons is not supported by the evidence presented to the Court.

[65] The Supreme Court of Canada did not in fact conclude that the existence of an expectation of privacy depends on the potential to draw intrusive conclusions from the information analysed. Rather, the Supreme Court of Canada indicated that what matters most is the intended use for a specific purpose of that information. In short, the Court should not look at the potential intrusiveness of the information following analysis. Rather, the only appropriate option is to look at the level of intrusiveness of the granular information on its face (pre-combination and analysis). The correct approach is to look at the present circumstances only, not at the future potential level of intrusion. The fact that content is not retained and that associated data does not reveal core biographical information means that there is in fact no intrusion.

[66] More specifically, the AGC contends that common law jurisprudence in regard to section 8 permits the collection of associated data through the authority conferred by the warrant itself. It is the warrant conditions themselves that allow the CSIS to collect and retain the associated data. In regard to intrusions into the privacy of third parties, the AGC admits that their interests are indeed affected. But, case law permits an inevitable intrusion of privacy following a balancing between private and collective interests performed by the judge when deciding whether to grant the warrant or not. An intrusion of privacy does not necessarily render the authorization to collect information unreasonable; it also does not need to be minimized as the balancing has already been performed.

(3) Suggested Amendments to the Conditions

[67] The AGC finally proposes amendments to the warrant conditions templates which can be read in the “Factual Context” section at paragraphs 9 to 25. In general, the AGC contends that

the [redacted] assessment period found in the current warrant conditions is sufficient as it is tied to a high threshold for retention i.e. the "reasonable grounds to believe" used by the Court when determining whether to issue the warrant or not. The AGC proposes a longer period to deal with [redacted] as it will be seen in the "Practical Effects" chapter (beginning at paragraph 201.

[68] In regard to the [redacted] assessment period suggested by the *amici*, such a short period of time is unworkable in practice. No evidence was presented supporting the idea that a period shorter than [redacted] is workable; rather [redacted] is reasonable and appropriately protects third parties' privacy interests. Alternatively, if the Court rules otherwise, whether in regard to the retention period or in regard to the nature of the assessment made, the AGC requests a period of implementation of [redacted] in order to attempt to adapt to changes.

B. *Arguments of the Amici Curiae*

[69] The *amici* contend that the CSIS does not have the legal authority to collect or retain information that is not threat related. In practice, they argue that information unrelated to threats or to targets must be destroyed as soon as practicable.

[70] Contrary to the AGC's position, the *amici* submit that section 12(1) of the *CSIS Act* provides exclusive authority for the Service to collect and retain information in the course of its investigations of threats to the security of Canada. In addition, the scope of the authority to collect and retain information through the operation of section 12(1) is not expanded when a warrant is issued pursuant to section 21. It is irrelevant whether information was collected or

retained from the operation of a warrant or not; section 12(1) alone defines the authority of the Service to collect and retain information. The only information the CSIS is authorized by statute to retain is threat-related information following a warrant issued pursuant to both sections 12(1) and 21 of the *CSIS Act*.

[71] In addition, the use of the expression “third party information” by the CSIS and its counsel is misleading. Rather, only threat-related information should be retained; the provenance of the information does not matter. Information from parties other than targets will typically be unrelated to threats and thus un-retainable. Even so, non-threat-related information can also be generated by the target of a warrant and by those the target communicated with. The defining factor that ought to be used in determining whether information can legally be retained is not who is communicating but rather the existence of a threat to the security of Canada.

[72] The *amici* submit that incidental collection with a minimum period of analysis to determine whether the collected data is threat related or not is the only collection of non-threat-related information that falls within the meaning of “strictly necessary” as per section 12(1) of the *CSIS Act*.

(1) Section 12(1) Applies to Section 21

[73] In regard to whether or not the expression “strictly necessary” of section 12(1) applies only to the function of collection or also to the function of retention, the *amici* suggest that the words “must be threat-related” in section 12(1) clearly define the retention of information as the wording precludes the retention of information unrelated to a specific threat.

[74] Given that section 21(1) reads "[…] required to enable the Service to investigate a threat to the security of Canada", it is clear that CSIS's collection of information must be limited to the associated data linked to the threat specified in the warrant. If "associated data" is to be retained by the service, it can only be on the basis that the data is threat related.

[75] If a warrant defines the destruction of the content of communications but does not address the destruction of associated data, it does not mean that the retention of the associated data is authorized. This is especially true when a condition of the warrant relates to the destruction of certain types of information. In short, retention of the "associated data" might be authorized by section 12(1) if it is threat related, but if it is not threat related, CSIS has no legal authority to retain the information.

[76] In regard to the wording of the condition, which reads, in part, as "may assist in the investigation of a threat", the *amici* suggest that this wording should be interpreted as allowing the CSIS to assist in the investigation of a particular threat. The *amici* submit that to interpret "may assist in the investigation of a threat" as allowing the retained data to someday assist in the investigation of an undefined threat is erroneous. Put succinctly, the *amici* proposes that the Service only be authorized to retain information through the effect of a warrant when the information is threat related, as per the meaning of section 12(1).

[77] A warrant granted pursuant to section 21 of the *CSIS Act* is only a tool used to collect or retain information over the course of a section 12(1) investigation. It is only when the

information fits within the parameters of section 12(1) that section 21 confers on the CSIS the authority to collect or retain information linked to the threat identified.

(2) Arguments on Privacy Interests

[78] The *amici* disagree with the CSIS's conceptualization of the definition and scope of "third party information" as a category of persons [redacted] The current interpretation is too narrow for three reasons: (1) the constitutionally protected privacy rights of a large numbers of persons are disregarded; (2) the analysis of relevance is incorrectly grounded in the method used rather than the third-parties' reasonable expectation of privacy; and (3) the issue is irrelevant, as the *CSIS Act* does not ask who the information comes from but rather whether if it is related to threats. In addition, they argue that privacy concerns of Canadians stand independently from section 12(1).

[79] The *amici* perform a substantial analysis of privacy interests related to section 8 of the Charter in their written submissions. In a nutshell, they posit that CSIS's collection and retention of information triggers section 8 protections as the collection and retention of information amount to a search and seizure. They argue that a reasonable, both subjective and objective, and strong expectation of privacy emanates from two sources: from the metadata itself, as it evidently shows private activity, and from the inferences that may be drawn from aggregating and analysing that same metadata. According to case law, the expectation of privacy of the public is normative (what society is willing to accept) and not descriptive (a conclusion derived from a particular factual matrix). The *amici* disagree with the AGC's position that granular metadata is meaningless information. The *amici* retort that jurisprudence supports their assertion

that information gleaned from granular metadata and from the product of its aggregation and analysis both generate information that goes to the "biological core" of a person and thus violates privacy. Metadata, on its own and processed through aggregation and analysis, can provide intimate insights into the lifestyle and personal choices of individuals; it is not an innocuous kernel of information. In addition, the products of the CSIS's analytical methods are much more elaborate than methods or types of information at issue in prior Supreme Court of Canada cases.

[80] The *amici* accept that a balance must be struck between the privacy interests of individuals and those of the state. According to them, the fine tuning of that balance can be struck by adjusting the retention period of the information collected.

(3) Suggestions Regarding Amendments to the Warrant Conditions

[81] The *amici*'s main proposal in regard to the warrant conditions is that the retention of information should be governed exclusively by whether or not the information collected is threat related. This categorisation aims to include information provisionally considered threat related through the mechanism of an assessment period. By definition, the *amici*'s proposal aims to exclude the retention of information that is discernably not threat related.

[82] The privacy rights of third parties must be upheld. While it is inevitable that their communications will be captured through the operation of warrants, the proper trade-off for this violation of privacy rights is that the retention of that information should be limited to a proportional period. In that regard, the *amici* propose specific definitions of terms and different

periods of retention for different types of information. Generally, the *amici* suggest that the Court allow information to be retained [redacted] in order for a communications analyst to make the determination of whether or not information is threat related. Before that determination is made, the information should be kept in a pre-analysis environment.

[83] For the *amici*, the difficulty lies not in clearly defining threat-related information, but rather in the treatment of ambiguous information. As a solution, the *amici* propose that a designated judge should set the appropriate period of retention at the warrant authorization stage on a case by case basis. If the judge does not set an appropriate retention period at that stage and if it is difficult to categorise the information as either falling within the ambit of the target of investigation or of a third party, then the CSIS must apply to the Court for directions following the collection of the information.

[84] As such, the *amici* notably propose changes to the warrant conditions governing the retention of third party information. First, the current period of retention of [redacted] generally ought to be reduced to [redacted] Incidentally, the *amici* suggest that the standard for retention should become "reasonable grounds to suspect" instead of the current standard "reasonable grounds to believe". In addition, associated data should not be distinguished from the content of the communication; both should be assessed and either destroyed or retained as a whole. Information, both content and metadata, should not be analysed until the information has been determined retainable or not. Finally, non-threat-related information should only be retained for the purpose of being disclosed in accordance with section 19 (Authorized Disclosure of Information) of the *CSIS Act*.

III. Issued raised

[85] The issues raised by the present application are the following:

1. Does the CSIS's omission to disclose and explain the existence of the ODAC program since its launch in 2006 amount to a behaviour breaching the duty of candour that the CSIS owes the Court?
2. If the collection function is to be performed only "[…] to the extent that that it is strictly necessary", does the "strictly necessary" limit also apply to the retention function in regard to information collected through the operation of warrants issued pursuant to sections 12(1), 2, and 21 of the *CSIS Act*?
3. Can the associated data, as defined at paragraphs 33-34 of these reasons, collected by the CSIS through the operation of warrants issued by this Court since 2006 be retained for future inquiries as part of the ODAC program pursuant to sections 12(1), 2, and 21 of the *CSIS Act*?
4. Are the amendments sought to the warrant conditions within the legal parameters set by sections 12(1), 2 and 21 of the *CSIS Act*?
5. What is the appropriate period of retention for information collected through the operation of warrants in order to permit the CSIS to assess whether the information may be of assistance to investigate a threat to the security of Canada, or may be useful in a prosecution, to international relations, or to the defence of Canada? If the information is assessed as being unrelated to any of these three objectives, when should it be destroyed?

## IV. Analysis

### A. *The Duty of Candour*

[86] I must determine whether the CSIS deliberately chose not to inform the Court, between 2006 and 2016, of its modified collection and retention policy in regard to warrants issued by this Court pursuant to sections 12(1) and 21 of the *CSIS Act*. I must also determine if such behaviour, in general, amounts to a breach of the CSIS's duty of candour towards the Court. I have briefly exposed some of the relevant facts to my analysis of the duty of candour at paragraphs 9 to 25 of these reasons.

[87] I have raised, on numerous occasions, at *ex parte, in camera* hearings, the issue of retention of information unrelated to threats or to the target of the warrant; many other designated judges have echoed this concern. The Court has proposed that such unrelated information be destroyed as soon as it is identified to be non-threat related. The Court has also suggested that the assessment period used to determine whether or not the collected information is threat or target related generally be limited to [redacted] and in some cases less. As an example, in file [redacted] the Court explored whether a retention period shorter than [redacted] was feasible.

[88] The designated judges have grappled with the issue of information unrelated to the threat or to the target before, notably when the Court dealt with [redacted] In that file, the Court decided that information such as [redacted] found to be unrelated to the investigation had to be destroyed within [redacted] A similar concern was also expressed in

regard to [redacted] warrants where a period [redacted] was determined in regard to [redacted] unrelated to the target of the warrant. Overall, the designated judges' approach to retention and destruction of third-party information has been consistent.

[89] The legal parameters of the duty of candour were detailed by Justice Mosley in *X (Re)*, 2013 FC 1275, later upheld on appeal in *X (Re*), 2014 FCA 249. Justice Mosley, at paragraphs 82 to 89, wrote:

> [82] The duty of full and frank disclosure in an ex parte proceeding was discussed by the Supreme Court of Canada in *Ruby v Canada (Solicitor General)*, 2002 SCC 75 (CanLII), [2002] 4 S.C.R. 3 at para 27:
>
> > In all cases where a party is before the court on an ex parte basis, the party is under a duty of utmost good faith in the representations it makes to the court. The evidence presented must be complete and thorough and no relevant information adverse to the interests of that party may be withheld; Royal Bank, supra, at paragraph 11. Virtually all codes of professional conduct impose such an ethical obligation on lawyers. See for example the *Alberta Code of Professional Conduct*, c.10, r.8.
>
> [83] The DAGC acknowledges that this duty, also known as the duty of utmost good faith or candour, applies to all of the Service's ex parte proceedings before the Federal Court: *Harkat (Re)*, 2010 FC 1243 (CanLII) at para 117, rev'd on other grounds 2010 FCA 122 (CanLII), appeal on reserve before the Supreme Court; *Charkaoui (Re)*, 2004 FCA 421 (CanLII) at paras 153, 154; *Almrei (Re)*, 2009 FC 1263 (CanLII), para 498. In making a warrant application pursuant to sections 12 and 21 of the *CSIS Act*, the Service must present all material facts, favourable or otherwise.
>
> […]
>
> [87] In *R. v. G.B.*, [2003] O.T.C. 785 (Ont. S.C.J.), a case involving an application for a stay of proceedings on the ground that a police officer had lied in affidavits to obtain wiretap authorizations, the Court described material facts as follows at paras 11 and 12:

> 11 . . . Material facts are those which may be relevant to an authorizing judge in determining whether the criteria for granting a wiretap authorization have been met. For the disclosure to be frank, meaning candid, the affiant must turn his or her mind to the facts which are against what is sought and disclose all of them which are known, including all facts from which inferences may be drawn. Consequently, the obligation of full and frank disclosure means that the affiant must disclose in the affidavit facts known to the affiant which tend to disprove the existence of either reasonable or probable grounds of investigative necessity in respect of any target of the proposed authorization.
>
> 12. The obligation of full and frank disclosure also means that the affiant should never make a misleading statement in the affidavit, either by means of the language used or by means of strategic omission of information.

[88] I agree with counsel for the DAGC that in the context of a warrant application pursuant to section 21 of the *CSIS Act*, material facts are those which may be relevant to a designated judge in determining whether the criteria found in paragraphs (21) (2) (a) and (b) have been met. […]

[89] However, I do not accept the narrow conception of relevance advocated by the DAGC in this context as it would exclude information about the broader framework in which applications for the issuance of *CSIS Act* warrants are brought. In my view, it is tantamount to suggesting that the Court should be kept in the dark about matters it may have reason to be concerned about if it was made aware of them. […]

[Emphasis added.]

(See *X (Re)*, 2013 FC 1275; and *X (Re)*, 2014 FCA 249)

[90] The Supreme Court of Canada, in *Canada (Citizenship and Immigration) v Harkat*, [2014] 2 SCR 33, 2014 SCC 37, at paragraphs 101 and 102, citing *Ruby v Canada (Solicitor General)*, 2002 SCC 75, [2002] 4 SCR 3, and *Almrei (Re)*, 2009 FC 1263, [2011] 1 FCR 163,

confirmed that an elevated duty of candour applies when a party relies on evidence in *ex parte* proceedings and that ongoing efforts to update the information are required.

[91] The CSIS began retaining associated data in 2006. From that time until December 2011, the Court was not informed by the CSIS that such information, unrelated to threats or to the target designated in the warrant, was being retained on an indefinite basis. In December 2011, at a hearing, CSIS alluded to the retention of data when discussing changes to the wording of the warrants. The purpose of the modification to the wording of the warrants, as explained by counsel for CSIS, was to "improve the vocabulary".

[92] There is documented evidence showing that from 2006 to 2008, the CSIS had every intention to inform the Court of its retention of associated data program. Thereafter, references to the CSIS's intention to inform the Court vanished, but there is no evidence clearly establishing that the CSIS deliberately did not intend to inform the Court. There is also no evidence to explain why the Court was not informed. No conclusive evidence on the matter has been presented to the Court.

[93] Having said that, the evidence establishes that as a result of the *Charkaoui II* decision of 2008, the CSIS reviewed its retention of information program and adapted its policies through the years. It is only in December 2011 that an amendment to the warrant conditions was effected to reflect the new retention policy of [redacted] applied only to "content" and implicitly not to "associated data".

[94] As briefly mentioned above, in the final moments of the December 2011 *en banc* hearing, which dealt with numerous amendments to the warrant conditions, counsel for the CSIS, upon being asked whether there was anything else to be raised, offered this last minute comment:

> "[…] there are other minor changes to the conditions that we think go to clarity […] we also looked at trying to better the language […] if I can put it that way; not change but to better the language, […] before it read as follows: "[…] subject to condition 1, any communication of a person" and now we have included the words "the content of any communication". "So it makes it clear the metadata is not part of what would be destroyed. And just so the Court is aware, basically the metadata is not destroyed and is retained no matter what happens to the communication except for solicitor-client which will be destroyed. […] Those are new changes that we made. It was really to reflect the practice and what other warrants are saying. We are always trying to better the language of the warrants."
>
> (See transcript of file [redacted] December 16, 2011 at 83-87.)

[95] The concepts of "metadata" and "associated data" were not the subject matter of the December 2011 *en banc* hearing. The Court, at the time, was dealing with other substantial changes to the warrant conditions template. The concept of retention and destruction of information was only broached in the final moments of the hearing, apparently to reflect an innocuous change to the CSIS's practice and "to better the language of warrants". In retrospect, this "minor change" was very far from minor and very far from simply "bettering the language".

[96] In June 2015, in file [redacted] which was heard over several hearings with the help of an *amicus*, I specifically brought up the issue of retaining third party information. Over those days of hearings, as the transcripts reveal, the CSIS never discussed its policy of retention of metadata. Yet, on numerous occasions, counsel for the CSIS told the Court that the issue of retention of third party information raised complex matters and that time was needed to reflect

on it. Over these six (6) hearings, I formulated several suggestions. First, warrant conditions should clearly express that non-threat, non-target information, such as third party information, should not be retained. Second, I suggested that the assessment period in regard to third-party information unrelated to threats and to the target should be limited to [redacted] and not [redacted] Counsel for the CSIS proposed to postpone these discussions so that the CSIS could review its own internal operations and submit new approaches at a later date. (See transcript of file [redacted] dated June 1, 2015 at page 55.) (See transcript of file [redacted] dated June 3, 2015 at pages 11-12.) (See transcript of file [redacted] dated June 10, 2016 at page 19.)

[97] As a result, on December 8, 2015, after two extensions of time granted by the Court, counsel for the CSIS submitted by letter a number of proposed amendments to the warrant conditions templates. The letter of December 8, 2015, did not divulge the Service's policy of retaining metadata. The amendments became the subject matter of file [redacted] The issue of CSIS's retention of metadata was only added to file [redacted] following the publication of the SIRC's 2014-2015 public annual report in late January 2016. It is only after reading the report and the letter of January 28, 2016, sent by the Deputy Attorney General that my fellow designated judges and I fully understood that the CSIS was retaining metadata. Following these events, it was decided that the policy of retention of such information would be added to the subject matters planned for the *en banc* hearing already called for to deal with the amendments described in the December 8, 2015 letter.

[98] In retrospect, I am concerned by the fact that both the CSIS and the SIRC knew of the retention program, but the Court did not. How can the Court properly assume its duties to assess

very intrusive warrants when the party appearing in front of it *ex parte* and *in camera* does not inform the Court of retention policies and practices directly related to the information the Court allows the CSIS to collect through the warrants it issues? The retention program was at the heart of the issues raised by the Court in file [redacted] yet the CSIS decided to ask for additional time rather than inform the Court of the existence of the program. I specifically note that the evidence shows the CSIS expressed the need to inform the Court of the details of the program as far back as 2006. Yet, it took extrinsic events for the Court to discover the existence of the program in 2016. Here are the relevant extracts of the 2014-2015 SIRC Report:

> "During a warrant application before the Federal Court in late 2011, when the matter of the wording change was raised, CSIS legal services did make reference to the retention of metadata. However, SIRC was given no indication that the Service was fully transparent with the Federal Court about the nature and scope of its activities with respect to metadata in the context of that discussion. SIRC, on the other hand, was of the view that the Court has a general interest in how the Service uses the intelligence, including metadata, collected under the authority of a warrant. […] SIRC therefore recommended that the Service make the Court aware of the particulars of the Service's retention and use of metadata collected under warrant. […] Given the continuing importance of this subject, the Committee will look more thoroughly at data exploitation and data acquisition in the next research cycle to assess whether collection is done "to the extent that is strictly necessary," as set out in section 12 of the *CSIS Act*."
>
> (Canada, Security Intelligence Review Committee, *SIRC Annual Report 2014-2015: Broader Horizons: Preparing the Groundwork for Change in Security Intelligence Review*, (Ottawa: Public Works and Government Services Canada, 2015) at p 25.)

[99] I note the important fact that the SIRC recommended to the CSIS that it inform the Court of its retention program, but that the CSIS refused to do so. It refused for the following reasons:

> "CSIS RESPONSE TO RECOMMENDATIONS: The Service did not agree with SIRC's recommendation to advise the Federal Court of activities relating to metadata collected under warrant. CSIS's

> position is that section 21 of the *CSIS Act* does not confer any general supervisory authority to Federal Court judges, therefore, it believes that SIRC's recommendation was both inappropriate and unwarranted. Moreover, the Service maintains that its position on the issue in question was communicated clearly and transparently to the Federal Court during a warrant application in December 2011. […]" [Emphasis added.]
>
> (Canada, Security Intelligence Review Committee, *SIRC Annual Report 2014-2015: Broader Horizons: Preparing the Groundwork for Change in Security Intelligence Review*, (Ottawa: Public Works and Government Services Canada, 2015) at p 26.)

[100] How can a privileged party, appearing on an *ex parte, in camera* basis, reply in such a way? Designated judges serve as the gatekeepers of intrusive powers, ensuring a balance between private interest and the state's need to intrude upon that privacy for the collective good. They must also ensure that the intrusive means sought are proportionate with the gravity of the threat. The warrants issued by the designated judges have direct impacts on the activities of the CSIS and on the information that can or cannot be collected and retained. Given its unique position as applicant and sole source of evidence to the Court, the CSIS has an elevated duty to ensure the designated judges can fully assume their role. The response provided to the SIRC's recommendation by the CSIS shows a worrisome lack of understanding of, or respect for, the responsibilities of a party benefiting from the opportunity to appear *ex parte*. If the CSIS unduly limits the flow of information the Court needs to make proper determinations, then the CSIS can be seen as manipulating the judicial decision-making process.

[101] In 2005, a CSIS task force recommended the establishment of a data retention program. From the day the program was implemented in 2006, the CSIS deemed the program important

enough to inform the Minister of its existence; the Service did so by letter in July 2006. At the time, the CSIS opined that the Court should also be properly informed:

> "[…] the Service will make a presentation to the Federal Court or in some other form, raise with the Court, the Service revised position on retention, and seek its comments on the matter […]"
>
> (See Affidavit of [redacted] dated April 21, 2016 at para 27.)

[102] If the retention program warranted such a presentation and asking the Court for comments back in 2006, then why did the CSIS only dismissively broach the topic at the end of the hearing in December 2011 under the guise of "bettering the language"? How can the CSIS credibly claim to have informed the Court "clearly and transparently"?

[103] I absolutely disagree with the CSIS's suggestion that the Court was informed "clearly and transparently". The CSIS knew, as far back as 2006, that it had to inform the Court of the substantial changes it brought to its policy of retention of information. Unfortunately, the evidence is inconclusive as to whether or not the CSIS intentionally did not inform the Court in a clear and transparent manner. At the very least, the CSIS was aware that it should inform the Court in 2006, yet did not do so.

[104] In addition, the CSIS's response to SIRC's recommendation to inform the Federal Court raises more red flags:

> "[…] CSIS's position is that section 21 of the *CSIS Act* does not confer any general supervisory authority to Federal Court judges […]."
>
> (Canada, Security Intelligence Review Committee, *SIRC Annual Report 2014-2015: Broader Horizons: Preparing the Groundwork for Change in Security Intelligence Review*, (Ottawa: Public Works and Government Services Canada, 2015) at p 26.)

[105] Such a position is unacceptable. How can the CSIS, in 2006, acknowledge the need to present the retention program to the Court and to seek its comments, but in 2015 claim that it has absolutely no responsibility to do so because the designated judges "have no supervisory authority"? This position is at the very least inconsistent and contradictory. It may also indicate that the CSIS in fact never intended to properly inform the Court at all.

[106] In the end, it took four (4) days of *en banc* hearings, several witnesses, and five affidavits for the CSIS to explain the associated data retention program and to answer the designated judges' questions.

[107] The CSIS has a privileged role to play with the Court; yet it cannot abuse its unique position. The CSIS cannot solely decide what the Court should and should not know. The CSIS, through its elevated duty of candour must inform the Court fully, substantially, clearly and transparently of the use it makes or plans to make of the information it collects through the operation of Court issued warrants. Failing to do so, the Court is in no position to properly assume its judicial obligation to render justice in accordance with the rule of law. The CSIS must have the confidence of the Court when it presents warrant applications. In the present file, it has certainly not enhanced the Court's trust.

[108] In its present submissions, at paragraph 99, the CSIS concedes that it has breached its duty of candour since 2006 in regard to the existence of the associated data retention program. The CSIS did not inform the Court "clearly and transparently" as it should have. Despite this admission, ten (10) years later, such behaviour remains unacceptable and runs contrary to the

interest of justice. For the purposes of this procedure, I find that the CSIS has breached its duty of candour by not informing the Court of its associated data retention program. In *X (Re)*, cited above, my colleague Justice Mosley, on a different factual basis, also concluded that a breach of the duty of candour had occurred. I make a similar finding three (3) years later. I wonder what it will take to ensure that such findings are taken seriously. Must a contempt of Court proceeding, with all its related consequences, be necessary in the future?

B. *Limited Mandate of the CSIS*

[109] I now begin the discussion on the interpretation of sections 12(1), 2 and 21 of the *CSIS Act* insofar as the collection and retention of information collected through the operation of warrants are concerned. I repeat that these reasons are limited to the application before me and to these sections only. In this section, I will ascertain in detail the primary mandate and functions of the CSIS. To do so, I will first perform a review of the applicable principles of legislative interpretation. Second, I will explore the context of the *CSIS Act*, notably by delving into the details of the events leading to the enactment of the Act. Third, I will thoroughly detail the scheme of the Act as that is crucial to properly resolve many of the issues at stake. Fourth, I will consider the differences and similarities with the *Charkaoui II* decision, cited above. Fifth and finally, I will spell out the key findings of this section.

(1) Principles of Interpretation

[110] In her book *Sullivan on the Construction of Statutes*, Prof. Sullivan sets forth the classic three-pronged method to interpretation: the ordinary meaning approach using the text of the

statute as the primary source, the contextual approach as originally described by Elmer Driedger and refined by the Supreme Court following its endorsement of the method in *Rizzo & Rizzo Shoes Ltd. (Re)*, [1998] 1 SCR 27, and the purposive approach in order to consider the practical idea behind the enactment of both the relevant section and the statute as a whole, as well as the real world effects of the Court's interpretation. (Ruth Sullivan, *Sullivan on the Construction of Statues*, 6th ed (Markham: Lexis Nexis, 2014) at para 2.1 ["Sullivan 2014"].)

[111] The Federal Court of Appeal, in *X (Re)*, 2014 FCA 249, at paragraphs 68 to 71, summarizes how a statute should be interpreted:

> [68] The preferred approach to statutory interpretation has been expressed in the following terms by the Supreme Court:
>
> > Today there is only one principle or approach, namely, the words of an Act are to be read in their entire context and in their grammatical and ordinary sense harmoniously with the scheme of the Act, the object of the Act, and the intention of Parliament.
> >
> > See: *Rizzo & Rizzo Shoes Ltd. (Re)*, 1998 CanLII 837 (SCC), [1998] 1 SCR 27 at paragraph 21. See also: *R. v. Ulybel Enterprises Ltd.*, 2001 SCC 56 (CanLII), [2001] 2 SCR 867 at paragraph 29.
>
> [69] The Supreme Court restated this principle in *Canada Trustco Mortgage Co. v Canada*, 2005 SCC 54 (CanLII), [2005] 2 SCR 601 at paragraph 10:
>
> > It has been long established as a matter of statutory interpretation that "the words of an Act are to be read in their entire context and in their grammatical and ordinary sense harmoniously with the scheme of the Act, the object of the Act, and the intention of Parliament": see *65302 British Columbia Ltd. v Canada*, 1999 CanLII 639 (SCC), [1999] 3 SCR 804, at para. 50. The interpretation of a statutory provision must be made according to a textual, contextual and purposive analysis to find a meaning

> that is harmonious with the Act as a whole. When the words of a provision are precise and unequivocal, the ordinary meaning of the words play a dominant role in the interpretive process. On the other hand, where the words can support more than one reasonable meaning, the ordinary meaning of the words plays a lesser role. The relative effects of ordinary meaning, context and purpose on the interpretive process may vary, but in all cases the court must seek to read the provisions of an Act as a harmonious whole.
>
> [70] This formulation of the proper approach to statutory interpretation was repeated in *Celgene Corp. v Canada (Attorney General)*, 2011 SCC 1 (CanLII), [2011] 1 SCR 3 at paragraph 21, and *Canada (Information Commissioner) v Canada (Minister of National Defence)*, 2011 SCC 25 (CanLII), [2011] 2 SCR 306 at paragraph 27.
>
> [71] Inherent in the contextual approach to statutory interpretation is the understanding that the grammatical and ordinary sense of a provision is not determinative of its meaning. A court must consider the total context of the provision to be interpreted "no matter how plain the disposition may seem upon initial reading" (*ATCO Gas and Pipelines Ltd. v Alberta (Energy and Utilities Board)*, 2006 SCC 4 (CanLII), [2006] 1 SCR 140 at paragraph 48). From the text and this wider context the interpreting court aims to ascertain legislative intent, "[t]he most significant element of this analysis" (*R. v Monney*, 1999 CanLII 678 (SCC), [1999] 1 SCR 652 at paragraph 26).

[112] As expressed by the Federal Court of Appeal, both Prof. Côté and Prof. Sullivan, in their most recent works, proclaim that the ordinary meaning approach by itself is no longer sufficient. Rather, both leading authors agree that context is paramount and interpretation is legitimate even if the ordinary meaning seems clear. Prof. Côté indicates:

> "[…] [W]e want to note our profound disagreement with the idea that interpretation is legitimate or appropriate only when the text is obscure. This idea is based on the view, incorrect, that the meaning of a legal rule is identical to its literal legislative wording. The role of the interpreter is to establish the meaning of rules, not texts, with textual meaning at most the starting point of a process which

> necessarily takes into account extra-textual elements. The prima facie meaning of a text must be construed in the light of the other indicia relevant to interpretation. A competent interpreter asks whether the rule so construed can be reconciled with the other rules and principles of the legal system: Is this meaning consistent with the history of the text? Do the consequences of construing the rule solely in terms of the literal rule justify revisiting the interpretation? and so on."
>
> (Pierre-André Côté, *The Interpretation of Legislation in Canada*, 4th ed (Toronto: Carswell, 2011) at 268-269 ["PA Côté 2011"].)

[113] As such, even though section 12(1) of the *CSIS Act* does not pose significant difficulty in regard to its plain, literal meaning, we must look further. As Prof. Côté expressed, we must ascertain whether the ordinary meaning fits within the context and purpose of section 12(1) read in conjunction with section 2 and the statute as a whole. (Sullivan 2014, above, at paras 2.1., 2.2, 23.15, 23.17.)

[114] Given that the plain meaning rule is no longer considered an adequate interpretative method by itself, both Prof. Côté and Prof. Sullivan agree that the old rules refusing to admit certain extrinsic elements informing context must also be abandoned. In fact, both authors agree that extrinsic material is useful to the task of convincingly interpreting statutes. Although all extrinsic evidence is admissible, the authors signal that the role of the Court has shifted towards determining what weight, authority and value the interpreter should attribute to the various factors. (PA Côté 2011, above, at 47.) (Sullivan 2014, above, at paras 23.15, 23.17.)

[115] It is well recognized that legislative histories are useful extrinsic aids to ascertain the legislator's intent and the purpose of an Act. When analysing legislative history materials, Prof. Sullivan specifies that, generally "[…] [i]n a Parliamentary system of government, there is likely

to be a relatively small number of individuals whose intentions largely control the content of legislative initiatives. In the case of statutes, this would include the recommending Minister, who will reflect the views of Cabinet; it would also include the Parliamentarians who comprise a majority of the Committee that reviews the bill". Thus, the statements given by those relevant persons are much more useful than simple comments or debates from other Parliamentarians. The Supreme Court of Canada regularly relies on legislative history materials to ascertain the objectives of schemes created by statutes. (Sullivan 2014, above, at paras 23.67, 23.81, 23.83.) (PA Côté 2011, above, at 47.)

[116] Although commission reports do not represent the voice of sponsoring ministers or involved Parliamentarians directly, both Prof. Sullivan and Prof. Côté clearly opine that commission reports are useful and admissible. In fact, they regard commission reports as particularly helpful to the interpretation process and note that they were the first type of extrinsic supports to receive affirmation from the Courts. Prof. Sullivan explains:

> "Often legislation is preceded by the report of a law reform commission or similar body that has investigated a condition or problem and recommended a legislative response. Such reports typically review the research carried out by the commission, state its findings, describe the policy options explored and set out recommendations. The work is non-partisan and the conclusions are carefully reasoned. These features potentially make reports more reliable than the materials found in Hansard. In addition, commission reports often play a clear role in the preparation of legislation, in some cases a major role which potentially enhances their relevance and significance. Not surprisingly, then, commission reports were the first type of legislative history to be admitted by the courts in statutory interpretation cases. […]"
>
> (Sullivan 2014, above, at para 23.68.) (PA Côté 2011, above, at 455-456.)

(2) Contextual Approach

[117] I will now thoroughly assess the context surrounding the *CSIS Act*. To do so, it will be essential to refer to the principles of interpretation enounced above and to refer to the legislative saga leading to the present version of the *CSIS Act*. I have provided a brief summary of the legislative history at paragraphs 50 to 55 of these reasons. I will now delve into the topic in more detail.

[118] As established by Prof. Sullivan and Prof. Côté, a purely textual solution is no longer considered a full answer to interpretation. The text of the statute must reflect the purpose of the scheme as expressed by the legislator's intent. Accordingly, to confirm our approach in assessing the CSIS's mandate and functions, the Court must study the legislative genesis of the CSIS. To do this, it is essential to go back to the early 1980s, when the McDonald Commission issued its report on the predecessor of CSIS, the Intelligence Service of the RCMP. This report triggered much political debate, which ultimately resulted in the introduction of Bill C-157. That bill was then reviewed by a Senate committee resulting in the Pitfield Report. In response to the changes proposed by the Pitfield Report, the government of the day introduced Bill C-9, which with some minor amendments became the *CSIS Act* in 1984.

[119] The McDonald Commission brought forward the concern of imposing on an intelligence agency a limited mandate and the concept of "to the extent that it is strictly necessary". This recommendation was not followed in Bill C-157, which was the first bill introduced to create a Canadian intelligence service. Following its study of Bill C-157, the Pitfield Report

recommended that the mandate should be limited to what is “strictly necessary for the purpose of protecting the security of Canada”. The government of the day followed the Pitfield Report’s recommendation to “strictly limit” the service’s mandate, but did not add to Bill C-9 “for the purpose of protecting the security of Canada”. It was explained at the time that a precise definition of threats to the security of Canada (section 2) sufficed when referenced by section 12.

(a) *McDonald Commission*

[120] A principle of interpretation calls for identifying the wrong that the proposed legislation is attempting to remedy. Before delving deep into the details of the *CSIS Act*’s legislative history, it should be said that one of the most important recommendations of the McDonald Commission was to propose the establishment of a civilian agency, completely separate from the RCMP. The McDonald Commission acknowledged that the new agency must be girded in a new mindset, completely distinct from how a police organization operates, in order to avoid repeating past abuses.

[121] The McDonald Commission, issued in 1981, as a result of its investigation into the activities of the Intelligence Service of the RCMP, expressed serious concern about the RCMP breaking the law in the name of national security. In order to ensure that such illegal activities would not occur again, the McDonald Commission suggested that the mandate of a future intelligence agency be expressly defined and limited in order to restrain and deter illegal activities by members of the agency in the name of national security. It recommended the following:

> [45] […] We think a statutory clause stating the need to restrict the security intelligence activities to what is strictly necessary for the security of Canada would make it more likely that those who direct and carry out security work will keep in mind the danger to liberty which can result from an overly expansive interpretation of the security intelligence agency's mandate.
>
> **WE RECOMMEND THAT** the legislation establishing Canada's security intelligence agency contain a clause indicating that the agency's work should be limited to what is strictly necessary for the purpose of protecting the security of Canada and that the security intelligence agency should not investigate any person or group solely on the basis of that person's or group's participation in lawful advocacy, protest or dissent. […] [Emphasis added.]
>
> (Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Second Report: Freedom and Security Under the Law*, vol 1, Part V, (Ottawa: Privy Council Office, 1981) at p 443-444, para 45.)

[122] This is why the "strictly necessary" concept to the mandate was introduced. Its purpose was to remind the operational intelligence staff that there were limits to their actions and that the rule of law prevented an overly expansive interpretation of the agency's mandate.

[123] Additionally, in order to prevent excessive intelligence gathering, it was recommended that the mandate of the new service be specific:

> [190] […] But in the absence of a clearly defined mandate, there is a natural tendency for a security intelligence agency, no matter how good its analytical capabilities, to err on the side of excessive intelligence-gathering, lest it be faulted by government for not having intelligence when asked. Intelligence-gathering is not something that can be simply turned on and off like a tap. This is another reason for the importance of Parliament's establishing a coherent, comprehensive mandate for security intelligence activities in this country.
>
> (Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Second Report: Freedom and*

> *Security Under the Law*, vol 1, Part V, (Ottawa: Privy Council Office, 1981) at p 499, para 190.)

[124] Furthermore, the McDonald Commission detailed what it considered the proper functions of an intelligence service to be:

> [30] (c) The Act should positively identify the agency's basic function of collecting, analyzing and reporting intelligence about threats to national security and negatively establish the limits of the agency's operations by stipulating that it must not perform intelligence functions unrelated to threats to national security (as defined in the Act) nor perform executive functions to enforce security measures. Besides providing for its general function, there are a number of specific functions the permissible extent of which should be provided for in the statute. These are activities outside of Canada, liaison with foreign agencies and with provincial and municipal authorities, and the provision of security intelligence reports in programmes of security screening for public service employment, immigration, and citizenship. [Emphasis added.]
>
> (Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Second Report: Freedom and Security Under the Law*, vol 2, Part VIII, (Ottawa: Privy Council Office, 1981) at p 894, para 30(c).)

[125] The Commission therefore recommended as follows:

> "[31] …WE RECOMMEND THAT Parliament enact legislation vesting authority in an organization to carry out security intelligence activities and that such legislation include provision for: […]
>
> (c) the general functions of the organization to collect, analyze and report security intelligence and to be confined to these activities, plus specific authorization of certain activities outside Canada, liaison with foreign agencies and provincial and municipal authorities and of the organization's role in security screening programmes;"
>
> 5. WE RECOMMEND THAT all intelligence collection tasks assigned to the security intelligence agency by the government be consistent with the statutory definition of the security intelligence agency's mandate and that all legislation and regulations providing

> special powers or exemptions for security purposes be consistent with the definition of threats to the security of Canada in the legislation establishing the security intelligence agency." [Emphasis added.]
>
> (Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Second Report: Freedom and Security Under the Law*, vol 2, Part VIII, (Ottawa: Privy Council Office, 1981) at p 895, para 31. Also found at p 1067, para 5 of the *Summary of Recommendations*.)

[126] As it can be read, the primary functions of collection and analysis are identified along with others. The Commission clearly expressed the concern that the mandate of the intelligence agency must be limited. Specifically, the primary functions must be consistent with the definition of threats to the security of Canada.

[127] The McDonald Commission addressed the retention of information separately from the other two primary functions (collection and analysis). The Commission, fully cognizant of privacy concerns and of the intricacies of an intelligence investigation, expected that the intrusive methods used would be proportionate to the gravity of the threats:

> "(b) The investigative means used must be proportionate to the gravity of the threat posed and the probability of its occurrence. In a liberal society, which as a matter of principle wishes to minimize the intrusion of secret agencies into the private lives of its citizens and into the affairs of its political organizations and private institutions, techniques of investigation that penetrate areas of privacy should be used only when justified by the severity and imminence of the threat to national security. This principle is particularly important when groups may be subjected to security intelligence investigations although there is no evidence that they are about to commit, or have committed, a criminal offence." [Emphasis added.]
>
> (Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Second Report: Freedom and*

> *Security Under the Law*, vol 1, Part V, (Ottawa: Privy Council Office, 1981) at p 513, para 2(b).)

[128] In summary, it was also the Commission's view that intelligence agencies would gather more information than required by "spin-off or accidental by product." In a prescient observation, the Commission asserted that an agency should not retain information unrelated to threats or potential threats to the security of Canada. The Commission exhorted that controls be established to prevent this phenomenon:

> [11] A further source of confidential information which might be available at this level of investigation is information received 'accidentally' through intrusive techniques which have been authorized for the investigation of another subject. The F.B.I. control system permits the use of existing human sources at this stage but not existing technical sources (i.e. electronic eavesdropping). We are dealing here with one aspect of the so-called 'spin-off' or accidental by-product phenomenon which will be discussed more fully in the next chapter. It is possible, for instance, that an authorized full investigation of organization A may yield information indicating that organization B may pose a serious threat to security, but a full investigation of organization B using intrusive techniques has not been authorized. In these circumstances, the system for controlling the use of intrusive investigative techniques could in effect be by-passed through exploiting this opportunity to use the incidental by-products of these techniques. Members of the agency at the field or desk level should be able to use this information in their preliminary appraisal of organization B but the use of information obtained in this way must be recorded at Headquarters, so as to facilitate the monitoring of the activity by the agency's senior management and by the independent review body.
>
> (Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Second Report: Freedom and Security Under the Law*, vol 1, Part V, (Ottawa: Privy Council Office, 1981) at p 517, para 11.)
>
> [14] We believe that controls are needed to prevent a security intelligence agency from maintaining files on thousands of people who are not threats or potential threats to the security of Canada. To say that the agency can collect information regarding

> individuals as long as this information relates to the agency's mandate is so vague and loose a rule as to justify almost any collection programme. […] [Emphasis added.]
>
> (Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Second Report: Freedom and Security Under the Law*, vol 1, Part V, (Ottawa: Privy Council Office, 1981) at p 518, para 14.)
>
> [21] The senior management of the security intelligence agency should maintain a sound programme of file review to extract material which in no way relates to the agency's mandate, or is no longer of use, so that it can be destroyed. The R.C.M.P. Security Service has maintained such a programme in recent years. Between January 1972 and June 1977, for instance; while 501,000 new files were opened, 332,201 were destroyed. Of course, as the destruction of the files relating to Operation Checkmate indicates there is a potential for abuse in destroying as well as in opening files. We have encountered instances in which instructions have been given to destroy files in order to obliterate any record of questionable activities. File destruction 'should not be carried out in an ad hoc manner but according to clearly established schedule and based on criteria approved by the Minister responsible for the agency. [Emphasis added.]
>
> (Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Second Report: Freedom and Security Under the Law*, vol 1, Part V, (Ottawa: Privy Council Office, 1981) at p 521, para 21.)

[129] Overall, the McDonald Commission urged that the mandate and collection and retention functions of the intelligence agencies be strictly limited to threats to the security of Canada. As a result, the Commission wanted the retention function to also be limited to what is "strictly necessary" in order to prevent retention of information unrelated to threats. The Commission went further: it recommended establishing policies ensuring such non-threat-related information be reviewed and destroyed. The Court's warrants conditions have tried to reflect these concerns.

[130] Before proceeding to the next stage relevant to establishing context, it is appropriate to consider the basic reasons for establishing legal parameters to the work of intelligence agencies. Legal parameters aim to prevent intelligence officers from acting illegally in the name of a so called higher interest. The Commission clearly expressed that national security matters do not permit intelligence officers to justify any action, no matter how illegal, by invoking the national security of Canada:

> [21] […] [T]he rule of law must be observed in all security operations. Several meanings have been given to this phrase. The meaning which we have in mind is that expressed by the English writer, A.V. Dicey, when he wrote that
>
> > […] every man, whatever be his rank or condition, is subject to the ordinary law of the realm and amenable to the jurisdiction of the ordinary tribunals […]. With us every official, from the Prime Minister down to a constable or a collector of taxes, is under the same responsibility for every act done without legal justification as any other citizen.
>
> In our context this means that policemen and members of a security service, as well as the government official and Ministers who authorize their activities, are not above the law. Members of the security organization must not be permitted to break the law in the name of national security. <u>If those responsible for security believe that the law does not give them enough power to protect security effectively, they must try to persuade the law-makers, Parliament and the provincial legislatures, to change the law</u>. They must not take the law into their own hands. This is a requirement of a liberal society. It is, therefore, unacceptable to adopt the view, which we have found expressed within the RCMP, that when the interests of national security are in conflict with the freedom of the individual, the balance to be struck is not for the court of law but for the executive. […] [Emphasis added.]
>
> (Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Second Report: Freedom and Security Under the Law*, vol 1, Part II, (Ottawa: Privy Council Office, 1981) at p 45, para 21.)

[131] This message resonates today as much as it did back when it was first put on paper. It is a reminder that we must stay vigilant in order to ensure that the legislative mandates of our security agencies are fully respected. If those mandates require changes, change must be brought through legislative amendment, not by stretching the language of an Act. In other words, modifications must be legitimately enacted by convincing the parliamentary branch of government that legislative amendments are required to enhance the collective security of Canada.

[132] I agree that in order to maintain and sustain the rule of law, the specific mandate of an intelligence agency must be clearly defined through legislation. The Commission identified the past wrongs and suggested ways to neutralize them. Some of these wrongs have been mentioned here. It is evident from the above excerpts of the Commission's report that establishing a defined mandate for the agency was a precise tool to correct these wrongs.

(b) *Bill C-157 and the Pitfield Report*

[133] As briefly mentioned earlier, Bill C-157 did not include the "strictly necessary" concept within the section on the duties and functions of the intelligence agency. Rather, the "strictly necessary" concept resulted from the review of Bill C-157 by the Senate (the Pitfield Report) issued in 1983. Bill C-157 was later reintroduced as Bill C-9. I notice from debates and reports that Bill C-157 was generally heavily criticized by commentators and witnesses; the vagueness of the original legislative mandate was critiqued.

[134] The Pitfield Report essentially established a workable framework for the creation of an intelligence service; most of its recommendations were followed and included in Bill C-9. Two crucial recommendations from the report for our purposes are: (1) the insertion of the "strictly necessary" concept in relation to the functions and mandate of the intelligence agency; and (2) the importance placed on the idea that the mandate of the agency be related to "threats to the security of Canada" and to the "protection of lawful advocacy, protest and dissent", as long as those actions are not related to the definitions of threat categories. What is most important to note is the emphasis placed by the Pitfield Report on the need for limitations to what is called the "primary function" (section 14 in C-157, then section 12, now section 12(1)) and on the idea that this function is circumscribed by the definitions of "threats to the security of Canada" (section 2).

[135] Here is how the Pitfield Report referred to the McDonald Commission and how it approached the mandate and functions of the future intelligence agency:

> [28] What might be termed the "primary function" of the proposed agency is to be found in s. 14(1) of the Bill:
>
> > The Service shall collect, by investigation or otherwise, 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.
>
> This subsection, on its face, is unobjectionable. <u>It sets out clearly what the principal activity of any security intelligence agency should be: investigation, analysis and the retention of information and intelligence on security threats</u>. This, of course, then leads to a very important question, the answer to which is crucial to the scope of the agency's power: what constitutes "threats to the security of Canada"? <u>In brief, how is the agency's mandate to be defined?</u>

[29] Before addressing this question, however, the Committee feels that it would be useful to stipulate an immediate limitation on the primary function in section 14. It has in mind what the McDonald Commission recommended, and what several witnesses endorsed: that there be included in the statute words which would indicate that the agency's mandate should not be given an overly expansive interpretation. The McDonald Commission suggested, in part, the following:

> that the legislation establishing Canada's security intelligence agency contain a clause indicating that the agency's work should be limited to what is strictly necessary for the purpose of protecting the security of Canada … (Recommendation 4, p. 443, Second Report)

[30] Adding words to this effect to s. 14(1) would, we believe, have a salutary effect on its interpretation. The recommendation in that Report also went on to include words which are found in s. 14(3) of the Bill. The Committee is of the opinion that this formulation is also useful, but that it should be expressed affirmatively, and within the definition of security threats, as discussed below.

[31] This, then, brings us back to the question of mandate. Section 2 contains the definition of "threats to the security of Canada". One cannot overstate the importance of this definition. It constitutes the basic limit on the agency's freedom of action. It will establish for the CSIS, its Director, and employees the fundamental standard for their activities. It will enter crucially into judicial determination of whether a particular intrusive investigation technique can be used. And it will provide a benchmark for assessment of agency activities by review bodies, and by the agency's political masters. It will not, however, create a crime or crimes.

[Emphasis added.]

(Senate of Canada, Special Committee of the Senate on the Canadian Security Intelligence Service, *Delicate Balance: A Security Intelligence Service in a Democratic Society*, (November 1983) (Chair: P.M Pitfield) at paras 28-31.)

[136] The purpose of the changes proposed in the Pifield Report was to "sharpen" the focus of the activities of the intelligence agency and to protect lawful demonstration and expression of different points of view, while adequately informing the government of genuine threats to the security of the nation. Again, this strong language, from a second report dealing with the same subject matters, reaffirms the McDonald Commission's recommendations to limit the mandate of the intelligence agency, only this time adding parliamentary senatorial input.

(c) *Bill C-9*

[137] On February 10, 1984, Mr. Robert Kaplan, the Solicitor General of Canada at the time, [the "Minister"] explained in the House of Commons the objectives of the bill and how they could be achieved:

> **Mr. Kaplan**: […] We want to restrict the mandate of our Security Service in order to define more clearly, and in greater detail, the scope of our security intelligence activities. We want to indicate the exact powers the Service will be authorized to use, and we want to specify conditions and limits of use of those powers. We want these conditions to be defined within a detailed framework that will ensure full respect for the law, and we intend to establish a non-governmental and fully independent committee that will monitor the justification of security intelligence activities and report regularly to the Solicitor General of Canada and to Parliament. The purpose of this Bill is therefore, to a large extent, to provide a new set of guarantees and controls that do not exist at the present time, in order to protect the rights of Canadians against undue interference. […] [Emphasis added.]
>
> (Canada, House of Common Debates, 24th Parl, 3rd Sess (10 February 1984) at 1272.)
>
> **Mr. Kaplan**: […] The new organization must at least be told, in the form of clear and unambiguous legislation, what it is supposed to do. That is why the proposed mandate is such an important part of Bill C-9. This mandate will be a definition by Parliament of the scope and limits of security intelligence activities. […] The primary purpose of the service will be to collect and analyze

> information and threats to Canada's security. […] The primary purpose of the service will be restricted to the collection, analysis and reporting of security intelligence. […] [Emphasis added.]
>
> (Canada, House of Common Debates, 24th Parl, 3rd Sess (10 February 1984) at 1273.)
>
> **Mr. Kaplan**: […] I should also point out that the mandate, as reworded in the Bill before you, limits all security investigations to those that are "strictly necessary", in the interests of national security. That is a clear signal that the mandate is to be interpreted narrowly. Only if it is demonstrably necessary for national security will an investigation be supported by this mandate. [Emphasis added.]
>
> (Canada, House of Common Debates, 24th Parl, 3rd Sess (10 February 1984) at 1274.)

[138] The words of the Minister are clear:

1. The legislative mandate of the security service is to be restrictive and is to be interpreted narrowly;
2. The legislative mandate will determine the scope of the security service's activities;
3. The powers given to the intelligence agency will be precise and limited;
4. The primary purpose of the service is to collect, analyse, and report information about threats to the security of Canada. I note that retention is not mentioned, although it is present in section 12 of the draft bill; a clarification will follow.

(d) *Standing Committee on Justice and Legal Affairs*

[139] At the Standing Committee on Justice and Legal Affairs, over a period of three (3) days, opposition members of Parliament, Mr. Lawrence (a former Progressive-Conservative Solicitor-General) and Mr. Robinson (a New Democratic MP from the province of British-Columbia),

specifically questioned the Minister on the wording of the proposed section 12. They asked whether the expression “to the extent that is strictly necessary” aimed to limit only the function of collection or also limited the function of retention of information. This is how the debate on this important issue evolved:

> **Mr. Allen Lawrence**: […] The FBI has to use what they call “minimization procedures” to reduce the degree of the invasion of the privacy to innocent persons. For instance, there has to be the prompt destruction of tapes, of personal conversations of innocent persons, who may have used the tapped phone. There is no such requirement, that I can find, in your bill. I would suggest to you that if you have not considered it, it should be.
>
> **Mr. Robert Kaplan**: It is a firm policy that information that is not relevant to the information that is collected properly, is destroyed.
>
> **Mr. Lawrence**: I am glad to hear that. If it is firm policy, then there is nothing wrong with putting a statutory requirement in about it, is there?
>
> **Mr. Kaplan**: Well, it is policy, so it could be in a statute. […]
>
> (House of Commons, *Minutes of Proceedings and Evidence of the Standing Committee on Justice and Legal Affairs*, 32nd Parl, 2nd Sess, No 28 (April 3, 1984) at p 10:54 (Chair: Claude-André Lachance).)
>
> **Mr. Svend Robinson (Burnaby)**: […] The clause includes the words “to the extent that it is strictly necessary.” Those words qualify “shall collect by investigation or otherwise”. It has been suggested by witnesses that they should in fact qualify all of the activities, the duties and functions of the service. I do not understand why that would not be the case. So they should “collect by investigation or otherwise and analyze and retain to the extent that is strictly necessary.” In other words, they would not be retaining information and intelligence except that which is strictly necessary to retain, or analyzing except to the extent it was strictly necessary to do so.
>
> I guess I am particularly concerned about retention of information and intelligence now. I will just ask the Minister for his preliminary views on that at this point. Given the unfortunate abuses that have occurred with respect to retention of information

and opening of files that should never have been opened, I would hope that the Minister would not be opposed in principle to a suggestion that the strict necessity test should also apply to the analysis and retention function as well as the collection function.

**Mr. Kaplan**: Well, I had followed in this amendment the exact recommendation of the Senate committee. The Senate committee looked at the function of collection as the one that ought to be limited to what is strictly necessary. We do not want them to collect any more than is strictly necessary because it is the collection that is the potential violation of people's privacy and rights.

**Mr. Robinson (Burnaby)**: And the retention. If they retain…

**Mr. Kaplan**: No but if you are limited at the entrance, should you not be able to analyze stuff that is properly collected more than to the extent strictly necessary? The analytical function has its own logic. If you have properly gotten the information and not violated people's privacy and rights in getting it, how can you say that the analysis of that should also be limited? I mean the analysis should be the analysis that the human mind can apply.

[Emphasis added.]

(House of Commons, *Minutes of Proceedings and Evidence of the Standing Committee on Justice and Legal Affairs*, 32nd Parl, 2nd Sess, No 28 (May 24, 1984) at p 28:52 (Chair: Claude-André Lachance).)

**Mr. Robinson (Burnaby)**: I am particularly concerned about the retention element.

**Mr. Kaplan**: The same thing applies. If you are satisfied the collection was strictly necessary, then you do not need to qualify the retention. We do not want to have another stage of assessment, because it is not logical. If you have closed the door to material that is not strictly necessary, you do not have to qualify its retention.

**Mr. Robinson (Burnaby)**: The point is the collection can be done on reasonable grounds. That is a low threshold as I am concerned and will be subject to some discussion.

The collection can be done on reasonable grounds. It may then be found that information has been collected which is superfluous, that should not have been collected. That is why I am suggesting

that the retention should be subject to the strict necessity test as well.

**Mr. Kaplan**: If it is found that it is not strictly necessary then it should not have been collected.

**Mr. Robinson (Burnaby)**: That is the retention question. I will come back to that. […]

[Emphasis added.]

(House of Commons, *Minutes of Proceedings and Evidence of the Standing Committee on Justice and Legal Affairs*, 32nd Parl, 2nd Sess, No 28 (24 May, 1984) at p 28:53 (Chair: Claude-André Lachance).)

Mr. Robinson (Burnaby): […] First of all, Mr. Chairman, under the provisions of Clause 12 the service would: Collect, by investigation or otherwise, to the extent that is strictly necessary, and analyse and retain […]

(House of Commons, *Minutes of Proceedings and Evidence of the Standing Committee on Justice and Legal Affairs*, 32nd Parl, 2nd Sess, No 28 (June 7, 1984) at p 38:39 (Chair: Claude-André Lachance).)

**Mr. Kaplan**: Mr. Chairman, I agree with the objective of strictly controlling the service. I think the language proposed in the Bill does that, and I would like to reserve my comments on the amendments to explain why I feel each amendment is either not necessary or counterproductive. […]

**Mr. Robinson (Burnaby)**: […] I move the Clause 12 of Bill C-9 be amended by striking out lines 42 to 45 on page 6 and line 1 on page 7 and substituting the following:

> "12(1) The service shall collect, analyse and retain to the extent only that is strictly necessary information and intelligence respecting activities that may on reasonable and probable grounds be"

Mr. Chairman, in this amendment, which I would hope would commend itself to Members on the opposite side of the House in particular, what I sought to do is to ensure that it is not just in the collection of information that the test of strict necessity applies, but also that when we are dealing with the analysis and particularly the retention of information they retain only the information which is strictly necessary.

I would hope, Mr. Chairman, the Minister would recognize that, by qualifying just the words “shall collect … to the extent that is strictly necessary, and analyze and retain information”, there is at least an implication that the service would be able to retain information that is not strictly necessary for their purposes. All this would do, in effect, is move the qualification of strict necessity to qualify all the major function; that is, the collection, the analysis and the retention. […]

I have deliberately not changed in any other way the wording of the government’s proposal. All I have done is just ensure that the requirement of strict necessity would apply, as I say, particularly to the retention of that information, and if it were found that information had been collected which was not strictly necessary in the pursuit of the mandate, Mr. Chairman, indeed, that information would not be retained. But as I say, if it ever came to the hands of the judges or particularly the director of the service. They could say that he could only collect what is strictly necessary, but they do not say that he cannot retain information that is not strictly necessary for the purposes of the mandate.

So Mr. Chairman, it is a small amendment, but I suggest it is a very important amendment, in terms of making clear that the service is not to move beyond its scope of strict necessity in the areas that are outlined in Clause 12.(1). […]

(House of Commons, *Minutes of Proceedings and Evidence of the Standing Committee on Justice and Legal Affairs*, 32nd Parl, 2nd Sess, No 28 (June 7, 1984) at p 38:42 (Chair: Claude-André Lachance).)

**Mr. Kaplan**: I suggest to him that the language proposed, if it had been observed by the service, if it has been in effect at the time, would have avoided the retention of files, because they would never have been collected in the first place. So the expression adds nothing to the protection of the public. And, on the analytical, to limit “analytical”, to limit the human mind to analysis, to the extent strictly necessary, to me, is not meaningful. I can see collection being limited; retention consequentially is limited, but to say one can only analyse something to the extent strictly necessary seems to be meaningless. [Emphasis added.]

**The Chairman**: It is moved by Mr. Robinson that Clause 12 of Bill C-9 be amended by striking out lines 42 to 25 on page 6 and line 1 on page 7 and substituting the following:

> 12.(1) The service shall collect, analyze and retain to the extent that is strictly necessary information and intelligence respecting activities that may on reasonable and formal grounds be
>
> Amendment negative: nays, 5; yeas, 3."
>
> (House of Commons, *Minutes of Proceedings and Evidence of the Standing Committee on Justice and Legal Affairs*, 32nd Parl, 2nd Sess, No 28 (June 7, 1984) at p 38:44 (Chair: Claude-André Lachance).)

[140] I have included a lengthy excerpt of these important discussions in order to give the full context of the exchange. In their submissions, the Attorney General and counsel for the CSIS only included a fraction of this exchange. Contrary to their submissions, as it can be read above, the Minister did not reject outright the amendment proposing to include the "strictly necessary" qualifier to the retention function.

[141] Rather, from these exchanges, mainly between Mr. Robinson and the Minister, the issue raised in the present file was squarely addressed. When Mr. Robinson asked why the "strictly necessary" concept could not be read as applying only to the collection function but also to the retention and analysis functions, the Minister answered that since collection of information is limited to what is strictly necessary, it went without saying that the information falling outside the scope of strict necessity would not be retained.

[142] Mr. Robinson then asked the Minister to address the collection of superfluous information that should not have been collected. The Minister replied: "If it is found that is not strictly necessary then it should not have been collected". The Minister added that if collection

was limited, retention of what is not strictly necessary would "consequentially" be limited as well.

[143] The Minister addressed the analysis function differently. He said that if the information was obtained "properly", then the service's analysis of that information should not be restricted. Further, he specified that applying the "strictly necessary" qualifier to the analysis function would be limiting the human mind, which was not the desired outcome.

[144] In short, the Minister considered it unnecessary to strictly and expressly limit the retention function as it was already implicitly limited by the strict collection of information. Likewise, the analysis function could not be restricted as long as the underlying information had been legally collected. The argument that the "strictly necessary" does not apply to the retention of information function does not correctly reflect what the legislator expressly wanted.

[145] Ultimately, Bill C-9 returned to the House of Commons for third reading; many amendments were proposed but all ended up time allocated. The bill passed third reading without any major amendments in June 1984 and was proclaimed in two parts over the period of July and August 1984.

(e) *5-Year Review and the Government's Response*

[146] The *CSIS Act*, as enacted, provided for a parliamentary review and a government's response five (5) years after the enactment of the Act. The review was completed in September 1990 and the government's response was filed in February 1991. Both documents confirm

Minister Kaplan's schematic view of the Act and reflect the fact that the large majority of the Pitfield Report recommendations were followed.

[147] The Government's Response specifically referred to sections 12 (now 12(1)) and 2 as composing the "primary mandate" of the Service. In addition, I note that it also fuses the three functions of collection, retention, and analysis in one general primary function; the functions are not separate and are all subject to the limitations found in sections 12 and 2:

> "[…] The Service's primary mandate, relating to its core security intelligence role, is to be found in two provisions of the *CSIS Act*: the definitions of "threats to the security of Canada" outlined in paragraphs 2(a), (b), (c) and (d); and the description of the Service's duty to collect, analyze and retain information and intelligence on "threats to the security of Canada" outlined in section 12.
>
> The exercise of this mandate is conditioned by the limits and controls specified in sections 2 and 12 themselves, by Ministerial directions, and by the Service's own operational policies and procedures. In addition, certain powers employed by the Service are subject to the requirement to obtain a judicial warrant. […]
>
> The security intelligence collection activities of CSIS are also subject to limitations beyond the definitions contained in section 2. Two of these appear in section 12 and have a major impact on the Service's investigative activities.
>
> - CSIS must "have reasonable grounds to suspect" that activities constitute a threat before the Service may commence and investigation.
>
> - CSIS may only collect information or intelligence "to the extent that it is strictly necessary.""
>
> (Canada, Solicitor General of Canada, *On Course: National Security for the 1990s – The Government's Response to the Report of the House of Commons Special Committee on the Review of the Canadian Security Intelligence Service Act and the Security Offences Act*, (Pierre H. Cadieux – Solicitor General) (February 1991) at ch 5, p 37-39.)

[148] Regarding section 21 and the application for warrants permitting the use of intrusive investigatory measures, the 5-Year Report provided a succinct overview of the intended mechanism:

> "[9.6.1] The warrant application and approval process is governed by sections 21 to 28 of the *CSIS Act*. Section 21 requires that ministerial approval be obtained before an application for a warrant can be brought before a judge of the Federal court. The section also requires that the Director of the Service or any employee designated by the Minister have "reasonable grounds to believe" that a warrant is required to investigate a threat to the security of Canada or perform the Service's duties and functions under section 16 of the *CSIS Act* (i.e., collect information concerning foreign states and persons). It is important to recognize that the warrant provisions are qualified by the provisions of the *CSIS Act* where the mandates of the Service are described. Specifically, attention should be brought to section 12 of the Act which provides that: [Emphasis added.]
>
> > The Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyze and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada…"
>
> (Canada, House of Commons, Special Committee on the Review of the *Canadian Security Intelligence Service Act and Security Offences Act, In Flux But Not In Crisis – Report of the Special Committee on the Review of the CSIS Act and Security Offences Act*, (September 1990) (Chair: Blaine Thacker) at p 120-121.)

[149] I note the important passage of the Review Report which explicitly states that the section 21 warrant mechanism is not a standalone scheme isolated from the restrictions of other sections. Indeed, the report clearly states that the limits of section 12 directly apply to the warrant application procedure under section 21.

(3) The Scheme of the *CSIS Act*: Purposive and Textual Analysis

[150] The essential question, as brought forward by the parties, is whether the different parts of the *CSIS Act* operate independently from each other or not. The *amici* argue that section 12(1) enounces general principles and thus applies to the entire Act. On the other hand, the AGC and counsel for CSIS retort that it takes an explicit or implicit import of a section in one part of a statute to another in order for the section to have an effect in another part. Thus, section 12(1) being in Part I would not apply to the warrant process found in Part II.

[151] Bearing in mind the applicable rules of interpretation and the history of the issues at play, the mandate of the CSIS is limited in respect of the collection and retention of information obtained by the operation of warrants. The application of those rules confirms that the CSIS is mandated to retain information that is threat related, but may not keep associated data collected from the operation of warrants. Associated data is, in effect, metadata collected through the operation of a warrant of which the analogous content was assessed as non-threat related and destroyed. I will also explain further below why such a limited mandate fits squarely within the teachings of the Supreme Court of Canada expressed in *Charkaoui II*, cited above.

[152] In order to understand the *CSIS Act* and to interpret the CSIS's mandate, it is necessary to begin with a general overview of the statute and to pay specific attention to the CSIS's legislative jurisdiction pertaining to collection and retention of information stemming from section 12(1).

[153] First, the Federal Court of Appeal's assessment of the purpose of the *CSIS Act* in *X (Re)*, 2014 FCA 249 at paragraph 86, provides a good starting point to support the idea that strict controls are built into the scheme of the *CSIS Act*:

> [86] […] The need for strict controls on the operations of security intelligence agencies has long been recognized. In *Charkaoui v. Canada (Citizenship and Immigration)*, 2008 SCC 38 (CanLII), [2008] 2 S.C.R. 326 the Supreme Court considered the legislative purpose and guiding principles that attended the creation of CSIS. At paragraph 22 of the reasons the Court quoted from the report of the Special Committee of the Senate on the Canadian Security Intelligence Service to the effect that:
>
> > A credible and effective security intelligence agency does need to have some extraordinary powers, and does need to collect and analyze information in a way which may infringe on the civil liberties of some. But it must also be strictly controlled, and have no more power than is necessary to accomplish its objectives, which must in turn not exceed what is necessary for the protection of the security of Canada. (Report of the Special Senate Committee, at para. 25)

[154] Second, the mandatory 5-year report following the enactment of the *CSIS Act*, issued in 1990, titled *In Flux But Not In Crisis – Report of the Special Committee on the Review of the CSIS Act and Security Offences Act*, provides a succinct overview of the operation of the Act at paragraphs 2.1 to 2.3:

> "[2.1] The Canadian Security Intelligence Service (CSIS) is a civilian agency controlled and managed by its Director under the direction of the Solicitor General. The Service does not have law enforcement powers and, as an intelligence agency, is not authorized to engage in offensive or "countering" activities. This means that its employees do not have the powers of peace officers to collect criminal evidence or effect arrests and that its activities are largely defensive in nature. CSIS has both a primary mandate and several secondary mandates.

> [2.2] The Service's primary mandate is established by section 12 of the *CSIS Act*. It is required to collect, by investigation or otherwise, to the extent that is strictly necessary, and to analyze and retain, information and intelligence about activities that are on reasonable grounds suspected of constituting a threat to the security of Canada. The Service reports to and advises the Government of Canada on these activities. Section 12 of the *CSIS Act* must be read in conjunction with the section 2 definition of "threats to the security of Canada". Threats to the security of Canada are defined as espionage or sabotage, foreign-influenced activities, terrorism and subversion. Under this definition, lawful advocacy, protest and dissent are not in and of themselves to be considered threats to the security of Canada unless carried on in conjunction with one of the elements of the definition. The combination of section 12 and the definition of threats to the security of Canada sets out the Service's security intelligence mandate.
>
> [2.3] The Service has three secondary mandates. They are set out in section 13, 14 and 16 of the Act."
>
> (Canada, House of Commons, Special Committee on the Review of the *Canadian Security Intelligence Service Act and Security Offences Act*, In Flux But Not In Crisis – Report of the Special Committee on the Review of the *CSIS Act* and Security Offences Act, (September 1990) (Chair: Blaine Thacker) at p 11-12, paras 2.1-2.3.)

[155] The government's response to the 5-year review report, titled *On Course: National Security for the 1990s – The Government's Response to the Report of the House of Commons Special Committee on the Review of the Canadian Security Intelligence Act and the Security Offences Act*, further enhances our understanding of the objectives of the statute at page 35:

> "[…] Under the *CSIS Act*, Parliament has assigned CSIS a clearly defined set of objectives. These are:
>
> - To collect, analyze and retain information and intelligence on activities that may on reasonable grounds be suspected of constituting threats to the security of Canada, in relation thereto, to report to and advise the Government of Canada (section 12);

> - To provide security assessments in support of the government's security clearance program (section 13);
>
> - To provide information and advice in support of government citizenship and immigration programs (section 14); and
>
> - To assist in the collection of foreign intelligence in Canada (section 16)."
>
> (Canada, Solicitor General of Canada, *On Course: National Security for the 1990s – The Government's Response to the Report of the House of Commons Special Committee on the Review of the Canadian Security Intelligence Service Act and the Security Offences Act*, (Pierre H. Cadieux – Solicitor General) (February 1991) at ch 5, p 35.)

[156] Third, on a more structural level, the *CSIS Act* is composed of four (4) parts and of a set of essential definitions which are linked to some of these parts. I will first elaborate on the four (4) parts and, when necessary, link them to relevant definitions.

[157] Part I pertains to the establishment of a civilian Canadian security intelligence service. Part II establishes and describes the judicial control mechanism applicable when warrants are sought by the CSIS. Part III establishes civilian oversight of the activities of the CSIS through the creation of the Security Intelligence Review Committee [SIRC]. Finally, Part IV provided for review of the function and operation of the entire scheme after five (5) years following the enactment of the Act. As covered earlier, such a review was performed, a report was filed, and the government issued a response. As a side note, when enacted in 1984, the *CSIS Act* also included ministerial control of the activities of the CSIS through the Office of the Inspector General. This function was abolished in part in 2012 and was not replaced.

[158] From this very general schematic description, in regard to warrants, it is immediately obvious that the legislator intended to ensure the activities of the CSIS would not be exclusively supervised by the judiciary. Indeed, the scheme also provides for supervision by both civilians (SIRC), and politicians (initially the Inspector General reporting to the Solicitor General, and later the Minister of Public Safety and Emergency Preparedness).

(a) *Ascertaining the Primary and Secondary Functions of the Service*

[159] Part I of the Act addresses the normal administrative set-up of a civilian agency, and also establishes and qualifies the duties and functions of the Service. The "primary function", to investigate threats to the security of Canada, is defined as such in the Pitfield Report and is established at section 12(1) (section 12(1) was originally section 14(1) in its predecessor, Bill C-157, and then section 12 before recent amendments). The Pitfield Report refers to section 12(1) as the "principal activity of any security intelligence service agency […]", such principal activity being "[…] investigation, analysis and the retention of information and intelligence on security threats". (Senate of Canada, Special Committee of the Senate on the Canadian Security Intelligence Service, *Delicate Balance: A Security Intelligence Service in a Democratic Society*, (November 1983) (Chair: P.M Pitfield) at p 11, para 28.)

[160] This "primary function" is complemented by the definition of "threats to the security of Canada" elaborated in section 2. Taken together, section 12(1) and section 2 form the core of the CSIS's essential function: investigate threats to the security of Canada.

[161] When conventional means of investigation do not allow to meaningfully advance an investigation, sections 21(1), 21(2), and specifically 21(2)b) [further referred to simply as "section 21"] come into play to allow the CSIS to apply for warrants before the Court. The application must show, on reasonable grounds, that the information sought is factually related to a threat to the security of Canada as referred to in sections 21(1), 12(1), and as defined in section 2. The affidavit in support of the warrant application and the examination that follows at the hearing are determinative for the designated judge charged with deciding whether to issue the warrant or not. As the Pitfield Report rightly noted when discussing this primary function, the definition of the threats to the security of Canada at section 2 of the Act:

> "[…] constitutes the basic limit on the agency's freedom of action. It will establish for the CSIS, its director, and employees the fundamental standard for their activities. It will enter crucially into judicial determination of whether a particular intrusive investigative technique can be used." [Emphasis added.]
>
> Senate of Canada, Special Committee of the Senate on the Canadian Security Intelligence Service, *Delicate Balance: A Security Intelligence Service in a Democratic Society*, (November 1983) (Chair: P.M Pitfield) at p 12, para 31.)

[162] Section 21 supports advancing an investigation when conventional means are not sufficient and intrusive methods are necessary. The role of the Court, in such cases, is to ensure all requirements of the legislation are respected in the application for warrants and that the measures sought are justified in light of the facts put forward. Section 21 does not create a separate scheme wholly distinct from the primary function of CSIS as described in section 12(1); rather, section 21 complements the primary function of "investigating threats" by establishing procedural requirements when an application for warrants is sought.

[163] As it can be read in section 21, an application for warrants must contain: the relevant facts; an explanation that other investigative methods were tried, but had either failed or are unlikely to succeed; the type of information to be intercepted; the identity of the target, if known, or classes of proposed targeted persons; a general description of the place where the warrant is to be executed; the proposed duration of the warrant; and any previous application for a warrant made by CSIS in relation to a person identified in the affidavit.

(b) *Details on the Secondary Functions*

[164] Having established that the essential function of the CSIS is to investigate threats to the security of Canada, I must now delve further into the secondary functions of the Service in order to fully grasp the scheme of the Act. The secondary functions of the CSIS are also detailed in Part I. They involve activities such as: providing security assessments to departments of the Government of Canada, to provinces, and to police forces (subsections 13(1) and 13(2) respectively); allowing the CSIS to enter into arrangements with foreign partners (section 13(3)); and providing advice to ministers of the Crown on matters related to the security of Canada (section 14).

[165] Notably, section 16, also included in the secondary functions, allows the collection of information concerning foreign states or persons in relation to the defence of Canada or to the conduct of international affairs. Canadian citizens, permanent residents, and Canadian or provincial corporations are excluded from section 16's ambit. The purpose of a section 16 investigation is to collect, within Canada, information or intelligence related to the capabilities, intentions, or activities of any foreign state, groups of foreign states, or any representatives

thereof. Justice Mactavish interpreted section 16 of the *CSIS Act* in *Canadian Security Intelligence Service Act (Re)*, [2014] 2 FCR 514, 2012 FC 1437 at para 84:

> [84] Subsection 16(2) of the Canadian Security Intelligence Service Act clearly prohibits the provision of assistance by the Service in response to a ministerial request, where that request is directed at [a Canadian citizen, permanent resident or corporation]. A [Canadian citizen, permanent resident or corporation] is a target of the warrants sought here. As a consequence, I am satisfied that I do not have the jurisdiction to issue warrants authorizing the Service to intentionally intercept the communications of, or utilize investigative techniques in relation [a Canadian citizen, permanent resident or corporation], including […]

(See also Canada, House of Commons, Special Committee on the Review of the *Canadian Security Intelligence Service Act and Security Offences Act*, In Flux But Not In Crisis – Report of the Special Committee on the Review of the *CSIS Act* and Security Offences Act, (September 1990) (Chair: Blaine Thacker) at p 11-12, para 2.3 for details.) (See also House of Commons, *Minutes of Proceedings and Evidence of the Standing Committee on Justice and Legal Affairs*, 32nd Parl, 2nd Sess, No 28 (3 April, 1984) at p 10:13 (Chair: Claude-André Lachance).)

[166] As it can be read in section 21, intrusive warrants may be sought for the purposes of section 16. But, contrary to warrants sought for the purposes of section 12(1) (relating to threats to the security of Canada at section 2), warrants sought through the application of section 16 in conjunction with section 21 requirements do not have to show a nexus to threats to the security of Canada. Rather, the alternate safeguard in place is that section 16 warrants may only be sought after either the Minister of Defence or the Minister of Foreign Affairs personally requests permission to do so from the Minister of Public Safety and Emergency Preparedness; who must agree.

(c) *Distinguishing the Effects of Section 21 on Sections 12(1) and 16*

[167] I must absolutely specify, again, that the determinations made in the case at hand, as well as the interpretation given to section 12(1) through these reasons, deal solely with the collection, retention, and analysis of information concerning the primary function identified (nexus with "threats to the security of Canada"). Interpretation of the secondary functions is not part of the issues raised in this application and no evidence has been presented on this matter.

[168] In short, section 21 relates to both sections 12(1) and 16, but as noted above, one is related to a threat to the security of Canada (section 12(1) in conjunction with subsection 21) while the other is related to gathering foreign intelligence following requests from ministers (section 16 in conjunction with section 21). Sections 12(1) and 16 must be dealt with differently as they are anchored in distinct factual bases when seeking an application for warrants. It can also be said that section 21 exists to procedurally enable the application of sections 12(1) and 16 through judicially authorized warrants. The other functions cannot avail themselves of the section 21 procedure.

[169] An investigation pursued under section 12(1) must respect the requirements established by section 21 to obtain intrusive warrants. Section 21 does not enlarge the primary function of section 12(1), rather it establishes procedural and evidentiary requirements to satisfy a designated judge that the intrusive warrants sought can be granted legally. (See House of Commons, *Minutes of Proceedings and Evidence of the Standing Committee on Justice and*

*Legal Affairs*, 32nd Parl, 2nd Sess, No 28 (10 April, 1984) at p 12:45 (Chair: Claude-André Lachance).)

(d) *Judicial Control Emanating from Section 21*

[170] In my view, both the McDonald Commission and the Pitfield Report reinforce my conclusion that section 21 (formerly section 22 in Bill C-157) was enacted to establish an efficient system of judicial control over the warrant application process.

[171] The Pitfield Report was not satisfied with section 22 of Bill C-157 and suggested a rigorous set of controls for warrants. The standard requiring a judge to be "satisfied" was critiqued and the report therefore recommended a more rigorous standard. This recommendation was followed when the government changed the standard to "belief on reasonable grounds".

[172] At the risk of repeating myself, section 21 was not enacted as a distinct and independent scheme from the primary function created by section 12(1). Rather, it was enacted to ensure rigorous procedural requirements and to provide a checks and balance system through effective judicial control. Overall, the recommendations that led to the enactment of section 12(1) aimed to ensure that "[…] the gravity of the threat to the security or the need to collect foreign intelligence is such as to justify the intrusion into the privacy of those affected by the warrant […]". In addition, the report urged the inclusion of a fixed limit on the duration of warrants and suggested that judicial considerations on the warrant applications would be a benefit to "[…] the introduction of the warrant process." [Emphasis added.] (Senate of Canada, Special Committee of the Senate on the Canadian Security Intelligence Service, *Delicate Balance: A Security*

*Intelligence Service in a Democratic Society*, (November 1983) (Chair: P.M Pitfield) at p 21, at para 60, and at p 23, at para 66.)

(e) *Distinction Between "Reasonable Grounds to Believe" and "Reasonable Grounds to Suspect"*

[173] Understanding the distinction between "reasonable grounds to suspect" at section 12(1) and "reasonable grounds to believe" at section 21 proves crucial to properly appreciating the *CSIS Act* in regard to investigations and to obtaining warrants.

[174] The coexistence of two distinct standards for the various stages of investigation was clearly intentional, as excerpts from committee work on Bill C-9 in 1984 show. Mr. Kaplan was the Solicitor General at the time and Mr. Ted Finn was the Executive Director of the Security Intelligence Transitional Group, Department of the Solicitor General. Mr. Finn then became the first Director of the civilian CSIS following the transition. The following are excerpts from their testimonies before the Standing Committee on Justice and Legal Affairs in regard to Bill C-9.

> **Mr. Kaplan**: I feel that the standard provided in subclause 12.(1), that "reasonable grounds to be suspected of constituting threats to the security of Canada", is a significant threshold ensuring that non-threatening activities would not be put under surveillance and that this is the threshold appropriate for the activities of the security service. […]
>
> **Mr. Finn**: I would make just a brief comment if I may, Mr. Chairman, and say that in contrasting that test with the test contained in the warrant section, Clause 21, the language of subclause 21.(1) requires reasonable grounds to believe that the conduct constitutes a threat to the security of Canada.
>
> **Mr. Kaplan**: So in other words, before intrusive techniques can be resorted to, the additional test of subclause 21.(1) has to be reached. […]

> (House of Commons, *Minutes of Proceedings and Evidence of the Standing Committee on Justice and Legal Affairs*, 32nd Parl, 2nd Sess, No 28 (3 April, 1984) at p 10:41 to 10:43 (Chair: Claude-André Lachance).)

[175] Although not necessary for the present reasons, I note that the amendments of 2015 concerning measures to reduce threats to the security of Canada require "reasonable grounds to believe" and not "reasonable grounds to suspect" (section 12.1(1) of the *CSIS Act*).

(f) *Comments on Part III – Review Processes (SIRC and Bill C-22)*

[176] Having dealt with Part II (Judicial Control), I will now briefly explore Part III of the *CSIS Act*, which establishes the review processes and the supervision of the activities of the Service complementary to the supervision of the Court adjudicating warrant applications.

[177] First, the Federal Court hears applications for warrants *in camera* and *ex parte*. Before rendering its decision, the Court inquires as to the basis for the application by questioning the affiants and the counsel for the CSIS, as well as by weighing the evidence and the arguments. Intrusive measures must be carefully considered as they greatly invade the privacy of targets. The legislator is cognizant of such consequences and determined that judicial control was necessary to limit such powers. I note that judicial control is exercised in regard to the specific facts of each investigation, looking both at past events and at anticipating the consequences going forward. In contrast to after-the-fact review, the Court is aware of the live issues and concerns the CSIS faces in its daily activities and investigations of threats to the security of Canada.

[178] Second, outside of the courts, the current oversight responsibility is limited to the work of the SIRC, the civilian oversight body. The SIRC, composed of members of the Queen's Privy Council, reviews *ex post facto* (after the fact) the performance of the CSIS, directions issued by the Minister, arrangements entered into by the CSIS concerning security assessments with the provinces or foreign states, regulations, etc. The SIRC can also notably investigate: any activities of the CSIS to ensure compliance with legislation (section 40(1)); complaints against the CSIS (section 41); and denials of security clearances (section 42). It annually issues a report to the Minister of Public Safety and Emergency Preparedness and to Parliament (section 53). The SIRC can also issue a special report of its own volition or upon request of the Minister (section 54).

[179] The CSIS is thus subjected to both judicial controls when warrants are sought under sections 12(1), 21 and 16 and to civilian oversight by reviews of its activities by the SIRC. The legislator established such controls to ensure the *CSIS Act* remains within the boundaries established by legislation. The SIRC also annually reviews approximately five (5) warrant applications to ascertain whether CSIS correctly fulfilled its responsibilities. The involvement of the SIRC provides insight into the preparation of applications for warrants, into the process of information collection supporting the affidavits, and into the overall legal implications of the CSIS's actions. The work accomplished by the SIRC is valuable and this Court appreciates the reviews performed. The 2014-2015 annual report dealing with metadata collection through the actualization of warrants is a perfect example. The reports also contain statistics on the warrants issued by the Court on a yearly basis. This is useful information and it may be that the SIRC will give more information on this in the future.

[180] Third, as I have already noted, the position of the Inspector General, responsible for ministerial supervision, has been abolished. As I write these present reasons, Bill C-22, *An Act to establish the National Security and Intelligence Committee of Parliamentarians and to make consequential amendments to certain Acts*, has been introduced in the House of Commons. The bill's purpose is to create a committee composed of Parliamentarians which will be mandated to review "(a) the legislative, regulatory, policy, administrative and financial framework for national security and intelligence; (b) any activity carried out by a department that relates to national security or intelligence, unless the appropriate Minister determines that the review would be injurious to national security; and (c) any matter relating to national security or intelligence that a minister of the Crown refers to the Committee." It remains to be determined if this proposed bill will be adopted and, if enacted, how this new committee will function within the supervisory agencies already established and with the Courts. (Canada Bill C-22, *An Act to establish the National Security and Intelligence Committee of Parliamentarians and to make consequential amendments to certain Acts*, 1st Sess, 42nd Parliament, 2015.) Presently, the Minister of Public Safety and Emergency Preparedness is the person at the executive level who, among other responsibilities, issues ministerial directives, reviews the CSIS's internal operational policies, and answers to the House of Commons for any matters related to the Service.

### (g) *Section 12(1) Details*

[181] I reiterate that I am analysing the wording of section 12(1) of the *CSIS Act* specifically in regard to warrants; I am not commenting on the applicability of these reasons to other functions of the Service. Succinctly, section 12(1) of the *CSIS Act* establishes the primary functions of the

CSIS: it collects, analyses, and retains information and intelligence on activities that may, on reasonable grounds, be suspected of constituting threats to the security of Canada. Threats are defined in section 2 of the *CSIS Act*.

[182] Other notable but unrelated functions of the Service to the case at hand are, among others: security assessments (section 13); advice to the Ministers (section 14); investigative powers (section 15); and collection of information concerning foreign states and persons (section 16). Taken together, these functions reflect the legislative mandate bestowed upon CSIS by Parliament.

[183] Both section 12(1) and section 2 include clear restrictions. In the case of the primary functions delineated in section 12(1), the expression “to the extent that it is strictly necessary” establishes an important mandatory restriction to the functions of the CSIS. The terminology used shows that the purpose of the section was intended to be clear and without ambiguity. In regard to section 2, the wording at the end of the definitions of threats to the security of Canada “but does not include lawful advocacy, protest or dissent, unless carried out in conjunction with any of the activities referred to in paragraphs a) to d)” shows that legitimate activities (lawful advocacy, protest or dissent) are specifically excluded from the ambit of the Service. The mandate and functions of CSIS are thus not open-ended; rather, they are clearly limited by the vocabulary used to describe them.

[184] When read literally a reader may deduce that the “strictly necessary” wording in section 12(1), given its position in the sentence, only applies to the first primary function (collection)

and not to the other two (retention and analysis). Furthermore, the “and” following the “strictly necessary” may further give the impression that collection is to be performed on a strictly necessary basis while the other two functions of retention and analysis are not limited in such a way. Such is what a strict limited literary view may call for. But as the principles of statutory interpretation require us to do, we must go further.

[185] Section 12(1) must be read logically: if collection of information is performed on a strictly necessary basis, it goes without saying that retaining the strictly filtered information is permitted because the point of entry of the information is the strict collection process. Therefore, the retention function may only logically retain what has been collected in a “strictly necessary” manner. The same rationale applies in regard to the analysis function: if information is validly collected, only that strictly collected information is analysed. In those scenarios, there are no issues of limits to retention or analysis of the information because it has been legitimately collected pursuant to section 12(1) and section 2. However, if the CSIS collects information more widely than legally permitted, i.e. outside the scope of the warrant or unrelated to threats, then the information cannot be retained long-term nor can it be analysed, because it should not have been collected in the first place.

[186] Given the wording of section 12(1), the CSIS may only collect and retain information if it is obtained through investigations or otherwise and if the information falls within the boundaries set by sections 12(1) and 2. Legitimate targets are individuals or groups of interest that are, or potentially are, related to activities constituting threats to the security of Canada as defined by section 2 of the Act. The CSIS may obviously analyse this strictly collected and strictly retained

information to the full extent of its capacities. But, it is crucial to distinguish that incidental collection of non-target and non-threat related information does not form part of what is "strictly necessary" to collect. Therefore, non-target and non-threat third party information may only be retained for a short period of time in order to ensure that it is not related to national security. If, after such short time period, the information is determined not to be related to threats to the security of Canada as defined by section 2 of the *CSIS Act*, or of assistance to a prosecution, to national defence or international affairs, it must be destroyed.

[187] If the collection of information through the operation of warrants is limited to threat-related activities of targets, then it is justifiable that such information be retained for future use and analysis. The particular issue that arises in this procedure, with the evidence presented, is that a warrant operation, be it an intercept of a telecommunication or of a written communication, can gather more than what is directly related to the target of the warrant. Therefore, non-target and non-threat information may be collected as a corollary effect to the operation of the said warrant. However, collecting such information is not within the scope of the warrant and is not why the warrant was granted. A warrant is issued because evidence demonstrated that the target is engaged in activities related to a threat as defined by section 2 of the Act. A warrant does not provide permission to retain associated data when such information pertains to non-target and non-threat-related information subsequently assessed by the CSIS as being non-threat related or of no assistance to a prosecution, national defence or international affairs.

[188] The parameters set by section 12(1) do not permit the CSIS to retain non-target and non-threat information on a long-term basis. If the CSIS wants to retain such information that is not covered by its mandate, it must obtain the appropriate legislative changes that will allow such retention. The CSIS's strict statutory mandate is not respected when the service indefinitely retains information on non-target and non-threat parties collected through the operation of warrants correctly targeting threats to the security of Canada. Simply coming into contact with a targeted individual, a targeted group, or the individual's or groups' means of communication does not automatically transform a third-party into a legal target. Non-threat and non-target information collected due to a coincidence of time and events should not be retained for more than a short assessment period to determine whether it is threat related.

(4) Additional Considerations

(a) *Differences and Similarities with Charkaoui II*

[189] Contrary to what counsel for the AGC and the CSIS assert, the decision of the Supreme Court in *Charkaoui II* supports my conclusions that the function of retention is also moderated by the "strictly necessary" limit, and that section 21 is not an independent scheme operating in isolation from the restrictions of section 12(1). The *Charkaoui II* decision does not contradict this Court's interpretation of section 12(1). In *Charkaoui II*, which also dealt with the retention of information, following a legislative history analysis of section 12(1) similar to ours, the Supreme Court affirmed that information related to targets of investigation must be kept in its original format and must not be transposed into secondary documents if the original is destroyed

afterwards. When doing so, the Supreme Court confirmed that the CSIS's mandate must be interpreted narrowly, as defined by section 12(1) of the *CSIS Act*.

[190] The essential distinction between these reasons and the conclusions in *Charkaoui II* in regard to retention of information lies in the fact that the *Charkaoui II* decision, when read in its totality, clearly addresses the retention by the CSIS of operational notes properly collected based on its enabling statute, whereas the case before the Court today deals with non-threat and non-target information being collected. Thus, we must read paragraph 38 of *Charkaoui II* carefully and draw appropriate distinctions:

> [38] 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. […]

[191] The Supreme Court did not address the retention of information falling outside that scope of relevance to threats or to targets. As such, only the Supreme Court's general statement in regard to retention, at para 38, appears relevant to our purposes:

> [38] […] 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.

[192] The Supreme Court also referred to the important recommendations of the Pitfield Report regarding the limited mandate of the service at paragraph 22. It cited the following paragraph of the Pitfield Report to convey its understanding that, since the CSIS was to be granted broad

powers of investigation, its functions should be strictly related to the objective of protecting the security of Canada:

> "A credible and effective security intelligence agency does need to have some extraordinary powers, and does need to collect and analyze information in a way which may infringe on the civil liberties of some. But it must also be strictly controlled, and have no more power than is necessary to accomplish its objectives, which must in turn not exceed what is necessary for the protection of the security of Canada. (Report of the Special Senate Committee, at para. 25)"

[193] Furthermore, the Supreme Court confirmed that the *CSIS Act* reflects the recommendations of the McDonald Commission and of the Pitfield Report:

> [24] The *CSIS Act* reflects the organizational and operational principles recommended in the reports that preceded its enactment. It sets out the various duties and functions delegated to CSIS, including the following examples. CSIS is primarily responsible for collecting "information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada" (s. 12). […]

[194] In that same decision, the Supreme Court is also alert to the issue that the modern role of the CSIS has not remained stagnant since the enactment of its founding statute in 1984; I retain and consider this important detail in its overall analysis:

> [26] 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.

[195] I take away from the above paragraphs that information not legally collected by the service, i.e. falling outside the scope of the warrant or unrelated to threats to the security of Canada, must not be retained by the CSIS. On the contrary, information that is indeed linked to threats to the security of Canada or to the target of a warrant must be retained in its original state by the CSIS to comply with the protected rights under section 7 of the Charter.

(5) Key Findings of this Chapter

[196] The history preceding the enactment of the *CSIS Act*, keeping in mind the principles of statutory interpretation, allows me to conclude the following regarding the legislator's intent. In brief, as a result of its limited mandate and primary functions, for the purposes of section 12(1), 2 and 21, the CSIS is allowed to collect and retain, to the extent strictly necessary, information gathered by investigation or otherwise that is associated to activities related to the definition of "threats to the security of Canada". Therefore, the CSIS may collect and retain all information related to "threats to the security of Canada" but not information falling outside those specific parameters. Associated data, as assessed by the CSIS to be non-threat related, and of no assistance to an investigation, to a prosecution, to the defence of Canada, or to international affairs, stripped of its analogous content, is information that does not fall within the CSIS's limited mandate.

[197] More specifically, information collected by investigation or otherwise, accidentally or as spin-off, cannot be retained if it is found to be unrelated to "threats to the security of Canada". Such is the case regarding accidental or spin-off information unrelated to threats to the security of Canada or to the target, collected through the operation of issued warrants. The CSIS cannot

retain associated data as it is not empowered by law to do so, in plain words, it has no jurisdiction to do so.

[198] In regard to the analysis function, the Court can only agree with the views expressed by the Minister in 1984: as long as the information has been legally collected, it may be analysed to the full extent of the CSIS's abilities. The "strictly necessary concept" cannot logically apply to such a function other than by relying only on properly collected and retained information.

[199] Returning to the wording of section 12(1) of the statute, the AGC's argument that the "strictly necessary" concept only applies to the function of collection misses the point. All three functions are premised on the idea that only legally collected information is retained and analysed by the service. Section 12(1), as interpreted, is defined by one key component which overrides all primary functions: the "strictly necessary" collection. It flows directly from this initial strict limit to collection that the other two functions can operate unimpeded; the filter has already been applied. If the collected information does not meet the strict necessity criteria, all three functions are operating outside the CSIS's limited statutory mandate.

[200] This is the only way to interpret section 12(1) of the *CSIS Act*. Failing to give full effect to section 12(1) contradicts the purpose intended by the legislator. Adopting such an understanding of section 12(1) and of section 2 (definition of "threats to the security of Canada") gives full recognition to the limited mandate of the service. The rule of law is entirely recognized through such an interpretation.

C. *Practical Effects*

(1) Changes Sought to the Warrant Templates

[201] For the purposes of this section, it will be important to keep in mind, among others, the following documentation:

1. The Letter of [redacted] counsel for the CSIS, to the Court, dated December 8, 2015, proposing the changes to the warrant;
2. The affidavits, examinations, and cross-examinations of [redacted] (with supplementary affidavit), of [redacted] and of [redacted] (in general and on the application of the portability clauses);
3. The submissions of the AGC and of counsel for the CSIS, including the reply and the submissions of the *amici*.

[202] In the December 8, 2015 letter, the CSIS initially proposed six amendments to the warrant conditions. As a result of the *en banc* hearings, new amendments were sought. They are as follows:

- (A) new condition that would permit the Service to retain [redacted] warrant and the [redacted] warrant for a period of [redacted]
- (B) a new condition authorizing the service to retain [redacted] under the [redacted] warrant, [redacted] warrant, and [redacted] warrant;

- (C) a new condition specifically and explicitly governing the [redacted] for the [redacted] warrant and the [redacted] warrant;
- (D) a new condition stating that information destroyed pursuant to a warrant condition [redacted] by the service under the [redacted] warrant, [redacted] warrant, [redacted] warrant, [redacted] warrant, [redacted] warrant, and [redacted] warrant;
- (E) It was initially proposed that in the conditions of the warrants all references to "Regional Director or his Designate" be replaced by "Service Employee" to reflect the fact that during the period of validity of a warrant, different employees at different levels may conduct the assessment of warrant collected non-target information. Following the *en banc* hearing, the CSIS proposed new changes with alternate wording adapted to the three categories of determination found in the warrants;
- (F) In the [redacted] warrant, the CSIS proposes to remove condition 2 as it deems this condition is unnecessary for two reasons. First, because the information received under the authority of such a warrant will always relate to the target of investigation. Second, given that prior to issuing a warrant, a designated judge has to assess whether the Service has demonstrated that such a warrant is required, a further assessment post-collection is unnecessary; it is the opinion of the CSIS that only target information is collected and that therefore this condition is not applicable;
- (G) Similarly, in the [redacted] warrant, and the [redacted] warrant, it is submitted that there is no need to have a post-assessment of collected information since the information collected has to be related to an investigation of a

threat (for the [redacted] or to a target (for the [redacted] warrant;

- (H) For the [redacted] warrant, it is proposed that a new condition 3 be added to cover information that may be obtained pursuant to paragraph 2 of the warrant as there is no such provision presently;
- (I) A few stylistic changes dealing with the solicitor-client condition (replacing the words "any solicitor-client communication intercepted or obtained" with "any solicitor-client communication obtained" in the [redacted] warrant; the [redacted] warrant; the [redacted] and the [redacted] warrant) since these warrants do not allow for the interception of communications, a solicitor-client communication may only be obtained (e.g. the copy of a letter) and not be intercepted. The Service is also proposing all references to the word "obtention" be replaced by the words "[…] from the date it was obtained" for all warrants using the word "obtention". These two changes, with others, as it will be seen, have been agreed upon pursuant to a directive of this Court issued January 11, 2016.

[203] As a result of the four-day *en banc* hearings, the CSIS proposed further additional changes to the warrants:

- (J) Adding a definition of "associated data", reviewing the definition of "communication" and introducing new wording limiting the retention period of associated data of unreported third party or unattributed communication to [redacted]

(See Submissions of the Application at para 13.)

(a) *A New Condition for* [redacted] *for the* [redacted] *Warrant, and* [redacted] *Warrant*

[204] Presently, the CSIS must destroy [redacted] within a period of [redacted] from the time of collection, whether or not the communication has been assessed as threat related pursuant to condition 2 of the warrant. As the evidence establishes, it is not [redacted] Furthermore, it is also difficult to predict how much time and resources will be necessary to do so. The CSIS proposes that such [redacted] be retained for a maximum of [redacted] starting from the date of collection, [redacted] Only once [redacted] would the [redacted] assessment period for retention begin. If the Service wishes to retain [redacted] for a longer period of time, it would have to apply to this Court and seek authorization.

[205] In itself, [redacted] does not disclose substantial content. Therefore, the collection of such information does not raise issues in regard to establishing links, or not, to threats to the security of Canada. By its nature, [redacted] collected through the operation of a warrant automatically raises threat related concerns. Such information can fall within the scope of the definition of threats. The evidence has also shown that it is not an easy task to assess the time period necessary to [redacted]

[206] I conclude that the amendment sought is acceptable and that the retention period of [redacted] is acceptable. If the information [redacted] at the end of the period, it must be destroyed unless an application to extend this period is presented by the CSIS to the Court within the [redacted] period. Within the [redacted] period, once the information is [redacted] the CSIS has [redacted] from the time of the [redacted] to assess whether or not the information can be retained pursuant to the warrant conditions and the *CSIS Act*. If it requires a longer period of retention, the CSIS can present an application to the Court.

[207] I am aware that [redacted] This new provision is not to be used in any way as a loophole to justify the retention of more information than is necessary. Notably, [redacted] that is obviously unrelated to the target or to the threat may not be retained. In addition, this condition may not be used to trigger the assessment period at a convenient time for the Service following the lengthened period of retention [redacted]

(b) *A New Condition Authorizing the Retention of* [redacted] *for the* [redacted] *Warrant* [redacted] *Warrant, and* [redacted] *Warrant*

[208] For the CSIS [redacted]

[209] The Service obtains information [redacted]

[210] The CSIS proposes that the potential usefulness of information collected through the operation of warrants for [redacted] ought to be assessed at the same time as the assessment for relevancy to threats to or to target is performed.

[211] I conclude that the retention of [redacted] is appropriate as long as the CSIS remains barred from accessing [redacted] retention must be limited to [redacted]

(c) *A New Condition that Would Govern* [redacted] *for the* [redacted] *Warrant, and* [redacted] *Warrant*

[212] The CSIS suggests a new condition that would govern any [redacted]

[213] This amendment is proposed in order to maintain the integrity of the information [redacted]

[214] Because sections 12(1) and 21 warrants permit the collection and retention of target and threat-related information as defined at section 2 of the Act, the statutory language does not authorize the retention of information incidentally collected from non-targets unless such information can be related to the threat described in the issued warrant. Therefore, only [redacted] may be retained for future use, notably for additional investigation or forensic investigation.

[215] The information [redacted] unless found to be threat-related, cannot be retained for more than [redacted] at the

most. As I will detail shortly, the two-stage [redacted] to [redacted] retention and destruction period will apply if the information [redacted] obviously belongs to third-parties, is devoid of direct implications with the target, or is evidently not threat related.

[216] I believe that such an approach addresses the concerns expressed by both sets of counsel on this topic. I note that the applicant, in its reply and in response to submissions of the *amici*, distinguished and proposed for the first time, [redacted] Reflecting this concern requires a new condition to be drafted that will properly [redacted]

(See Applicant's reply submissions at para 87.)

(d) *Destruction of Information*

[217] The Court has imposed on the Service an obligation to destroy what is considered unimportant for the purposes of the investigation or what is unrelated to the targets named in the warrants. This obligation is found as a condition in various warrants.

[218] In application [redacted] Chief Justice Crampton raised, amongst other concerns, the definition of "destroyed" and the fact that the wording of the warrant did not capture that when information is deleted, it should mean permanently deleted and irrecoverable. [redacted] Therefore, this Court wants to ensure that [redacted]

[redacted] To reflect this reality, the CSIS is required to undertake that [redacted]

[219] Having said this and for the sake of utmost clarity, the undertaking should establish that the CSIS [redacted] nor will any other agency do so on its behalf.

(e) *Proposition Concerning Delegation and Accountability ("Regional Director or his Designate" to be Replaced by "Service Employees")*

[220] In the letter dated December 8, 2016 addressed to the Court, counsel for the CSIS initially proposed that wherever decision making responsibilities were entrusted to the Regional Director General or his Designate in the warrant conditions, the wording should be changed to entrust the responsibility to any "service employees" instead. This proposal raised numerous concerns from designated judges as voiced during the *en banc* proceedings and individual warrant applications since. As a result, the CSIS asked for time to ponder changes to its proposal. It was thereafter proposed that "Regional Director General or his Designate" be replaced with alternate wording to be adapted to three categories of determinations found in warrants templates dealing with [redacted] and warrant conditions.

(i) General Comments

[221] The Court was initially concerned with the appropriateness of delegating decisional responsibility from a clearly identified person to an unknown, unidentified employee. The Court

is concerned that such a change would negatively affect the accountability of the CSIS. The delegation of responsibility must be carefully effected; the present warrant conditions reflect this concern by requiring a top-ranking employee, either a “Regional Director General” or “his Designate” (e.g. someone specifically designated by the “Regional Director General”) to make the important selection in accordance with the warrants conditions.

[222] Warrants, by definition, are exceptional and intrusive means of investigation. Asking the Court to authorize the transfer of these important decision-making responsibilities to unidentified “service employees” as a category is inappropriate. The concept of accountability in such a situation is most important. To allow the transfer of such responsibilities to a category of unidentified CSIS employees would not serve to enhance accountability.

[223] As noted above, the CSIS nonetheless proposes that the wording “Regional Director General or his Designate” be adapted to the three categories of determination found in the warrants, i.e. [redacted] and warrant conditions. I will review each one keeping in consideration the different scenarios but also the evolving CSIS position on this matter.

(ii) [redacted]

[224] [redacted]

[redacted] Such work must be performed by an identifiable and fully accountable senior employee of the CSIS. (See affidavit of [redacted] dated May 24, 2016 and also his testimony of April 1, 2016 at p 49-82.)

[225] Such [redacted] can be found in the [redacted] warrant (paragraphs 3(g), 3(h), 3(i), 6(b), 6(e), and 13(f)) and in the [redacted] warrant (paragraph 1(b)) and in the [redacted] warrant (paragraph 1). In all of these cases, presently, the important decision of adapting the warrant to non-target [redacted] has to be made by one of the seven Regional Director Generals or his or her Designate.

[226] In my opinion, it is essential to ensure a senior executive of the CSIS, such as a Regional Director General, takes such an important decision. Allowing a senior executive to do so is appropriate because the delegation falls within the mandate of the identified executive pursuant to the *CSIS Act*; it does not violate the designated judges' mandate. But, I stress that for such a delegation to remain valid and legal, the information collected must remain related to the threat identified and the target of the warrant. (See *R. v Thompson*, [1990] 2 SCR 1111, 73 DLR (4th) 596, and also *Canadian Security Intelligence Act (Re)*, [1998] 1 FCR 420,file CSIS-36-97 (dealing with a visitor clause).)

[227] Now, the CSIS proposes to limit the authority to invoke a [redacted] to the Regional Director General personally. References to "Regional Director General or his

designate" would therefore be replaced with "Regional Director General" in all [redacted] This would apply to the warrants templates enumerated at paragraph 225 of these reasons. I agree.

(iii) [redacted]

[228] The [redacted] warrant (para 7e), the [redacted] warrant (para 4), and the [redacted] warrant (para 1d and 2) provide that a Regional Director General or his Designate may obtain [redacted] if, on reasonable grounds to believe, such information may assist in the investigation of a threat to the security of Canada.

[229] The *amici* raised valid concerns about the current wording of this condition and suggest new wording. The AGC and counsel for the CSIS have taken note of the *amici*'s proposal and have asked in their reply to delay the debate to a later warrant application in order to conduct a proper review of this power.

[230] I agree with the *amici* and the Chief Justice in file [redacted] and with some of my colleagues, for example in files [redacted] and [redacted] that the clause raises important concerns. Through this clause, the CSIS may obtain information related to Canadians who are not the target of a warrant. I am concerned by such a possibility. Until this matter is fully addressed, the Court will not renew such a clause. The Court shall await the CSIS's proposal on this matter.

### (iv) Further Changes from "Regional Director General or his Designate" to "Designated Service Employees" for the Task of Assessing Warrant-collected Non-target Information

[231] For the purposes of conditions 2, 3 and 4 of the [redacted] warrant; conditions 2, 3, 4 of the [redacted] warrant; conditions 2, 3 of the [redacted] warrant; condition 2 of the [redacted] warrant; condition 2 of the [redacted] warrant; and condition 2 of the [redacted] warrant, the CSIS proposes that the "service employee's" experience in effectuating the work related to the operation of a warrant be reflected in the warrant application. To that effect, the CSIS proposes the wording "Regional Director General or his Designate" be changed to "designated service employee". As the conditions require, the work required is to review and assess the collection of non-target information through the operation of warrants to ensure that only information that is useful to a threat investigation, may be of some use to a prosecution, or informative for national defence or international affairs is kept. The remaining information must be destroyed. Such a decision is important and must be taken by a knowledgeable person.

[232] The CSIS proposes the following definition for "designated service employee": "designated service employees means […] a service employee designated by the director or belonging to a class of employees designated pursuant to service policies to conduct assessments found in the warrant conditions and for which a regional director general or a director general is accountable of these employees actions".

[233] The evidence shows that, in practice, executing a warrant involves a team of CSIS employees with a variety of expertise and field-work experience. As the conditions of warrants

show, the collection of information often requires CSIS employees to assess information in order to determine whether it is threat related or not. Performing such assessments requires knowledge of the target's daily life, environment etc. A Regional Director General cannot realistically acquire distinct knowledge of each target the CSIS identifies [redacted]

[234] I agree that the warrant conditions must recognize operational reality and adapt to it. As long as accountability remains strong, notably with the ultimate responsibility resting on the shoulders of a Regional Director General, operational work dealing with the assessment of information collected through the operation of a warrant should be performed by the most relevant resource as long as such task is given to specific individuals and not a class of employees. It could thus refer to individuals as long as the Regional Director General remains fully accountable.

[235] Because the definition proposed in the warrant refers to "service policies", and because those policies become integral to the warrant, the Court asks the CSIS to forward to the Court, within thirty (30) days of such policies being finalized, on an ongoing basis, a copy of these policies in order for designated judges to review them. The judges will then determine whether the policies meet judicial requirements pursuant to section 21 of the *CSIS Act*. The amendments

being sought will be finally dealt with once the Court has had an opportunity to review the policies.

(f) [redacted] *Warrant Amendment to Remove Condition 2*

[236] The CSIS proposes to remove condition 2 because the information collected in this type of warrant only concerns the target of the warrant. Considering that a designated judge, at the warrant application, already assessed whether the records sought are required to investigate a threat to the security of Canada, the CSIS argues that there is no need to perform an assessment following the collection of the information.

[237] I agree with the spirit of this proposal but I will not modify the condition. Such a modification is only acceptable as long as the information collected always directly relates to the target. But, if by the simple operation of a warrant, information which may not relate to the target is collected, an assessment will still be required to ensure it does not relate to persons other than the target. Therefore, in order to reflect this concern, I will not remove this condition; condition 2 will remain unchanged.

(g) *Amendments to the* [redacted] *Warrant and* [redacted] *Warrant Concerning Condition 3*

[238] For the [redacted] warrant, the CSIS proposes that the scope of the current condition 3 (proposed new condition 4) be modified. Presently, information collected pursuant to part 4 is assessed following collection. However, the CSIS suggests that such a follow-up assessment is redundant as all the information collected under these types of warrants

falls under the “may assist in the investigation of a threat to the security of Canada” standard. I agree in part with this proposal: the condition dealing with [redacted] must remain; a new condition 4 must be added. It is my understanding that the CSIS is in agreement.

[239] Similar to the paragraph above, the CSIS proposes a modification to the scope of condition 3 as an assessment following collection pursuant to part 5 of the [redacted] warrant is unnecessary. The CSIS proposes that condition 3 remain as is in regard [redacted] obtained pursuant to part 6 of the [redacted] warrant. I agree with this proposal; a new condition 4 must be added.

(h) [redacted] *Warrant - New Condition 3*

[240] The CSIS proposes, since no condition deals with collection pursuant to paragraph 2 of the [redacted] warrant, that a new condition 3 be added to reflect the fact that an assessment is specifically performed following collection for [redacted] warrants. I agree with this proposal.

(i) *Solicitor-Client Clarifications and Other Changes, of Which Some Have Already Been Agreed Upon*

[241] This suggestion is made to ensure that the CSIS will not intercept solicitor-client communication. The CSIS suggests that the wording “any solicitor-client communication intercepted or obtained” ought to be changed to “any solicitor client communication obtained” in condition 1 of the [redacted] warrant, of the [redacted] warrant, of the [redacted] and of the [redacted] warrant. . The word “intercepted” is removed to reflect the fact that, following this change,

solicitor-client information may only be obtained and not intercepted. I already agreed with this proposal. This change was agreed following a directive issued January 11, 2016.

[242] As the word “obtention” is not commonly used in English, the CSIS proposes to replace it with “obtained”. Therefore, as already accepted in the directive issued, all references to “obtention” in the warrants are to be changed to “[…] it was obtained”. This has already been agreed to.

[243] The CSIS proposes that the current retention assessment period of [redacted] be brought down to [redacted] in regard to the [redacted] and [redacted] warrants. This has already been agreed to.

[244] The CSIS proposes that condition 2 of the [redacted] warrant be similar to condition 2 of both the [redacted] and [redacted] warrants to ensure consistency across the three warrants. I agree.

[245] Section 1 of the [redacted] warrant establishes limits as to what may be obtained, such as any record, document, or thing in the possession of a [redacted] Presently, these limits are excluded from condition 2 of the [redacted] warrant but they apply to both [redacted] and [redacted] warrants. Therefore, the CSIS proposes that the limits imposed by Section 1 become part of condition 2 of the [redacted] warrant. This change is proposed to promote consistency but also because an assessment post collection is required in limited situations.

[246] I agree, yet, I note that this is more than a stylistic change. The original wording requires that the CSIS review all information collected, including information concerning the target; if the information was assessed as unrelated to the threat then it must have been destroyed. Following this change, target related information will not be reviewed for destruction, only information related to non-targets will be.

(j) *Further Changes Sought Following the En Banc Hearings (New Definition for "Associated Data", Communication and Retention Period of [redacted] Rather than Indefinitely)*

[247] It is only as a result of the 2011 *en banc* hearing that selective wording was inserted to specify that the content of a communication may be destroyed. By performing this change, without properly informing the Court, the CSIS effectively distinguished content from associated data. Given that the condition implicitly rendered the warrant condition silent in regard to associated data, the CSIS interpreted that it could indiscriminately retain associated data indefinitely. From 2006 to 2011, the CSIS retained such associated data without the approbation of a warrant condition to this effect. In addition, following the "stylistic change" of 2011, the CSIS kept on retaining such information without having informed the Court fully and transparently of this retention.

[248] Following the *en banc* hearings and the concerns raised by the Court, the CSIS now proposes additional amendments. They include: defining "associated data", reviewing the definition of "communication", and as seen above, limiting the retention of associated data to [redacted] rather than indefinitely as it has been the case since 2006.

[249] There may be good reasons to review the definition of “communication” in light of the present reasons, but it may be better to do so at a later stage. Given my conclusions on the mandate of the CSIS, there is no need to address the proposal to limit the retention period of associated data to [redacted] associated data cannot be retained at all because it falls outside the CSIS’s legislated mandate.

[250] I have detailed above the reasons supporting my conclusion that the mandate and functions of the CSIS are strictly limited by legislation. Parliament, in 1984, legislatively established a civilian agency with a definite mandate and precise functions in order to prevent the reoccurrence of serious errors and abuses identified by the McDonald Commission. A proper interpretation of sections 12(1), 2, and 21 of the *CSIS Act* establishes that the primary mandate and function of the CSIS to investigate threats must be performed on a strictly necessary basis. Intrusive measures may only be used following the issuance of a warrant. The information collected through the operation of these warrants may only be retained if it is related to threats to the security of Canada as defined in section 2; associated data is not such information.

[251] As detailed in the Analysis portion of these reasons, the Court was and is concerned with the CSIS’s decision to retain associated data. Given my conclusion that the CSIS does not have jurisdiction to retain associated data unrelated to threats to the security of Canada, there is no need, at this time, to define associated data in the warrant conditions template. There is also no reason for the Court to make findings regarding the privacy expectations of individuals resulting from the retention of associated data. Following the same logic, it is unnecessary to weigh the state’s interests against private interests in regard to using associated data for investigative

purposes. These issues may again surface in future proceedings if the legal and factual contexts align.

(2) Further Comments–A Two Stage Process to Assess Warrant-Collected Information

[252] Given that associated data is not threat related, therefore falling outside the strictly limited primary mandate and functions of the CSIS, retaining such information indefinitely falls outside the jurisdiction of the Service. I have not reached this conclusion lightly. I understand the burden on time and resources the assessment pursuant to condition 2 imposes. I am aware that certain types of intrusively warrant-collected information can be assessed much more easily and much quickly than others. Notably, I am cognisant of the fact that [redacted] that certain formats are much harder to access than others; and that some information is obviously threat related while some is not.

[253] Given the amount of variables involved, I now propose two different assessment periods to process and assess warrant collected information. First, the CSIS will have [redacted] to assess information that is evidently not threat related and that does not involve the target. Second, information falling outside the scope of the first category must be assessed within a full [redacted] period (i.e. in the [redacted] following the initial [redacted] period). Following the respective performance of these assessments, information (both content and associated data) found to be of no assistance to an investigation of a threat, useless for prosecution, or unrelated to international affairs or the defense of Canada, must be destroyed. I do not consider that

implementing this two-stage approach creates an undue burden on the CSIS. A period of [redacted] from the date of these judgment and reasons is allowed for the CSIS to implement this two-step process of assessment. If more time is required, a motion requesting an extension can be presented to the Court.

## V. CONCLUSION

### A. *Conclusions Reached Regarding the Specific Issues Identified*

[254] The following are the conclusions I have reached in regard to the issues identified at para 85 of these reasons.

[255] First, in regard to the CSIS's duty of candour, I conclude that it had an obligation, beginning in 2006, to fully inform the Court of the existence of its collection and retention of associated data program. The CSIS also had the duty to accurately describe this program to the Court. The fact that it did not do so until 2016, other than alluding to it in December 2011 under the guise of "stylistic reasons", amounted to a breach of the CSIS's duty of candour. As a party appearing *ex parte* and *in camera* before the Court on a regular basis, the CSIS had an elevated obligation to inform the Court of the use it was making of non-threat-related information collected through the operation of warrants; it failed to do so.

[256] Second, I conclude that the qualifier "to the extent that it is strictly necessary" found in section 12(1) establishes that the CSIS's mandate is restricted. The CSIS's limited mandate incorporates the three functions of collection, retention and analysis of information. The qualifier

"to the extent that it is strictly necessary" applies not only to the function of collection but also to the function of retention. In addition, section 12(1) must not be read solely in conjunction with the definition of threats to the security of Canada as found at section 2 of the Act but also in conjunction with section 21. Section 21 is a procedural section which describes the threshold required that CSIS must meet in order to present an application to obtain intrusive warrants before a designated judge of the Federal Court. It also contains the pertinent components of a warrant application. Section 21 does not enlarge the scope of the jurisdiction given by legislation to the CSIS; its jurisdiction is clearly established at sections 12(1) to 16 in conjunction with the section 2 definition of threats to the security of Canada.

[257] Third, I conclude that the retention of associated data falls outside the CSIS's legislatively defined jurisdiction and does not respect the CSIS's limited primary mandate and functions.

[258] Fourth, the amendments to the warrant conditions template proposed by counsel for the CSIS in the letter dated December 8, 2015 and further developed at the *en banc* hearing are granted in part as detailed above. My previous conclusions obviously impact some of the amendments sought while other amendments have been specifically addressed.

[259] Fifth and finally, information collected through the operation of warrants must be assessed in order to determine whether it may assist with a national security investigation, may be of some use to prosecution, relate to international affairs or to the defence of Canada. The information thus collected must be assessed using the binary categorization test I have described

above: first, information obviously unrelated to the target of the warrant and unrelated to a threat to the security of Canada must be assessed within [redacted] of collection; second, information that falls outside the first category must be assessed within [redacted] following the end of the first period). For exceptional cases such as [redacted] the two-step [redacted] and [redacted] period applies only from [redacted]

B. *Closing Comments*

[260] I am fully cognizant of the consequences my decision has on the CSIS's mandate and functions; I have not reached these conclusions lightly. On the contrary, I have done my utmost to consider every possible way my conclusions may be wrong. Ultimately, the rule of law must prevail; without it, the actions of people and institutions cannot be trusted to accurately reflect the purpose they were entrusted to fulfil. Canada's legislation must be interpreted as intended by the legislator. If legislation limits the powers of an institution, these limits must be respected. A liberal interpretation of limits performed by the institution itself can only be stretched so far.

[261] The CSIS, a Canadian intelligence agency, is privileged to assume its duties using intrusive measures which would otherwise be illegal. The enactment of the *CSIS Act* was considered the best possible answer to the world order following the wars of the twentieth century, the Cold War and the FLQ Crisis. However, it was considered crucial to legislatively define and restrict the mandate of the CSIS in order to prevent the reoccurrence of abuses and errors committed by the CSIS's predecessor.

[262] In 1984, the legislator deliberately defined the “primary function” (section 12(1)) of the new CSIS in a limited fashion. The CSIS was tasked to collect information, on a strictly necessary basis, through the operation of warrants issued in response to a threat to the security of Canada (section 2); no more than that. As a result, the principle of strict collection must be reflected in the retention of that information. Since then, much time has passed and technology has considerably evolved. Technology behind the operation of warrants has progressed so much that the scope and volume of incidentally gathered information have been tremendously enlarged. The information gathered is vast but must still be carefully assessed in order to ensure that its collection and retention complies with the law. The evolution of technology is no excuse to flout or stretch legal parameters. When the information collected does not fall within the legal parameters delimiting the agency’s functions and actions, it cannot legally be retained. If the CSIS does indeed retain this illegal information, the Court must intervene and enforce compliance with the law.

[263] I am aware that other intelligence agencies operate differently and are able to adapt to new technologies and programs. Other agencies, whether domestic or foreign, are not necessarily subject to the same legal parameters as the CSIS. The fact that other agencies may operate more liberally and with less scrutiny does not allow the CSIS to unilaterally adapt its legislated mandate. Given that the CSIS’s mandate is defined in law, the statute governing its functions must be amended in order to permit the CSIS to operate differently if that is considered advisable by the legislator. The CSIS must be certain at all times that it holds the proper legislative authority to perform its activities.

[264] In *obiter*, considering the present reasons and the conclusions I have reached, subject to the appeal process, it may be time for Canadians to renew a debate regarding the mandate and functions of our domestic intelligence agency. As seen in the late 1970's and early 1980's, a similar debate proved fruitful. Although many different and opposing points of view were expressed, the Parliament of Canada managed to shepherd controversial issues into the enactment of the *CSIS Act* in 1984. The last thirty (30) years have shown that the enactment of the *CSIS Act* was a strong response to the intelligence challenges presented by the paradigms of the times. Yet it is my opinion that the *CSIS Act* is showing its age. World order is constantly in flux; for example state cyber-attacks are a novel form of war and a new era of the old Cold War is appearing. In addition, terrorist attacks are deeply hurting innocent civilians across the world, technology evolves rapidly, and priorities and opinions change. Canada can only gain from weighing such important issues once again. Canadian intelligence agencies should be provided the proper tools for their operations but the public must be knowledgeable of some of their ways of operating.

[265] Although I have determined in these reasons that the retention of associated data falls outside the legal scope of the *CSIS Act*, I think it important for future debates to note that evidence was produced establishing that the processing and analysis of associated data has yielded some useful intelligence results. In some cases, analysis of retained data in past cases indeed contributed to new investigative leads and other useful pertinent information. In addition, associated data in itself consists mostly of numbers associated to names; devoid of its analogous content, raw associated data may only have limited privacy impacts. Having said that, when the numbers and names are put together upon an investigative request, the intelligence product

resulting of the analysis may reveal more and therefore have a greater impact on privacy interests. It is not for me to decide whether or not such an invasion of privacy interests is outweighed by the State's legitimate interest in investigating threats, regardless of the quality of the intelligence produced. Another forum, or designated judges, may eventually be called upon to make further determinations on these matters.

[266] In addition, I have considered ordering the destruction of the associated data collected since 2006. I decided not to do so because of possible jurisdictional issues and because I did not benefit from submissions on this topic from both sets of counsel.

[267] Finally, coming to the end of these elaborate reasons, I repeat that the warrant templates are live documents which are adapted to reflect the ongoing concerns of ensuring that the intrusive measures authorized by the warrants are well controlled, scrupulously reviewed, and correctly directed at the target and the threat. Keeping in mind the operational needs and requirements of the CSIS, warrants should not involve innocent persons who benefit from full rights to their privacy. Designated judges must fully weigh these essential concerns to respect the rule of law. As usual, the CSIS is provided ample opportunity to request any changes and amendments it deems justified.

## JUDGMENT

**THIS COURT'S JUDGMENT is that**

- The CSIS has breached, again, the duty of candour it owes to the Court;
- The CSIS has a limited mandate which does not permit the retention of associated data, as defined at paragraphs 33-34 of these reasons, as it has done so since 2006, therefore this retention of associated data is illegal;
- The CSIS shall amend the warrant templates in accordance with the enclosed reasons;
- The present reasons shall be reviewed initially by the *amici curiae* to identify what parts of these judgment and reasons can be made public within seven (7) days of the date of the present judgment and reasons. After those seven (7) days, counsel for the Attorney General and for the CSIS shall review the redactions suggested within the subsequent seven (7) days. Any contentious issues shall be referred to the undersigned within the following three (3) days for determination.

"Simon Noël"

Judge

# VI. APPENDICES

## A. *Relevant Legislation*

| *Canadian Security Intelligence Service Act*, RSC, 1985, c C-23 | *Loi sur le Service canadien du renseignement de sécurité*, LRC, 1985, ch C-23 |
|---|---|
| **Judicial Control** | **Contrôle judiciaire** |
| **Application for warrant** | **Demande de mandat** |
| 21(1) If the Director or any employee designated by the Minister for the purpose believes, on reasonable grounds, that a warrant under this section is required to enable the Service to investigate, within or outside Canada, a threat to the security of Canada or to perform its duties and functions under section 16, the Director or employee may, after having obtained the Minister's approval, make an application in accordance with subsection (2) to a judge for a warrant under this section. | 21(1) Le directeur ou un employé désigné à cette fin par le ministre peut, après avoir obtenu l'approbation du ministre, demander à un juge de décerner un mandat en conformité avec le présent article s'il a des motifs raisonnables de croire que le mandat est nécessaire pour permettre au Service de faire enquête, au Canada ou à l'extérieur du Canada, sur des menaces envers la sécurité du Canada ou d'exercer les fonctions qui lui sont conférées en vertu de l'article 16. |
| **Matters to be specified in application for warrant** | **Contenu de la demande** |
| (2) An application to a judge under subsection (1) shall be made in writing and be accompanied by an affidavit of the applicant deposing to the following matters, namely, | **(2)** La demande visée au paragraphe (1) est présentée par écrit et accompagnée de l'affidavit du demandeur portant sur les points suivants : |
| (a) the facts relied on to justify the belief, on reasonable grounds, that a warrant under this section is required to enable the Service to investigate a threat to the security of Canada or to perform its duties and functions under section 16; | **a)** les faits sur lesquels le demandeur s'appuie pour avoir des motifs raisonnables de croire que le mandat est nécessaire aux fins visées au paragraphe (1); |
| (b) that other investigative procedures have been tried and have failed or why it appears that they are unlikely to succeed, that the urgency of the matter is such that it would be impractical to carry out the investigation using only other investigative procedures or that without a warrant under this section it is likely that information of importance with respect to the threat to the security of Canada or the performance of the duties and functions under | **b)** le fait que d'autres méthodes d'enquête ont été essayées en vain, ou la raison pour laquelle elles semblent avoir peu de chances de succès, le fait que l'urgence de l'affaire est telle qu'il serait très difficile de mener l'enquête sans mandat ou le fait que, sans mandat, il est probable que des informations importantes concernant les menaces ou les fonctions visées au paragraphe (1) ne pourraient être acquises; |

| | |
|---|---|
| section 16 referred to in paragraph (a) would not be obtained; | |
| (c) the type of communication proposed to be intercepted, the type of information, records, documents or things proposed to be obtained and the powers referred to in paragraphs (3)(a) to (c) proposed to be exercised for that purpose; | **c)** les catégories de communications dont l'interception, les catégories d'informations, de documents ou d'objets dont l'acquisition, ou les pouvoirs visés aux alinéas (3)a) à c) dont l'exercice, sont à autoriser; |
| (d) the identity of the person, if known, whose communication is proposed to be intercepted or who has possession of the information, record, document or thing proposed to be obtained; | **d)** l'identité de la personne, si elle est connue, dont les communications sont à intercepter ou qui est en possession des informations, documents ou objets à acquérir; |
| (e) the persons or classes of persons to whom the warrant is proposed to be directed; | **e)** les personnes ou catégories de personnes destinataires du mandat demandé; |
| (f) a general description of the place where the warrant is proposed to be executed, if a general description of that place can be given; | **f)** si possible, une description générale du lieu où le mandat demandé est à exécuter; |
| (g) the period, not exceeding sixty days or one year, as the case may be, for which the warrant is requested to be in force that is applicable by virtue of subsection (5); and | **g)** la durée de validité applicable en vertu du paragraphe (5), de soixante jours ou d'un an au maximum, selon le cas, demandée pour le mandat; |
| (h) any previous application made under subsection (1) in relation to a person who is identified in the affidavit in accordance with paragraph (d), the date on which each such application was made, the name of the judge to whom it was made and the judge's decision on it. | **h)** la mention des demandes antérieures présentées au titre du paragraphe (1) touchant des personnes visées à l'alinéa d), la date de chacune de ces demandes, le nom du juge à qui elles ont été présentées et la décision de celui-ci dans chaque cas. |
| **Issuance of warrant** | **Délivrance du mandat** |
| (3) Notwithstanding any other law but subject to the Statistics Act, where the judge to whom an application under subsection (1) is made is satisfied of the matters referred to in paragraphs (2)(a) and (b) set out in the affidavit accompanying the application, the judge may issue a warrant authorizing the persons to whom it is directed to intercept any communication or obtain any information, record, document or thing and, for that purpose, | **(3)** Par dérogation à toute autre règle de droit mais sous réserve de la Loi sur la statistique, le juge à qui est présentée la demande visée au paragraphe (1) peut décerner le mandat s'il est convaincu de l'existence des faits mentionnés aux alinéas (2)a) et b) et dans l'affidavit qui accompagne la demande; le mandat autorise ses destinataires à intercepter des communications ou à acquérir des informations, documents ou objets. À cette fin, il peut autoriser aussi, de leur part : |
| (a) to enter any place or open or obtain access | **a)** l'accès à un lieu ou un objet ou l'ouverture |

| | |
|---|---|
| to any thing; | d'un objet; |
| (b) to search for, remove or return, or examine, take extracts from or make copies of or record in any other manner the information, record, document or thing; or | **b)** la recherche, l'enlèvement ou la remise en place de tout document ou objet, leur examen, le prélèvement des informations qui s'y trouvent, ainsi que leur enregistrement et l'établissement de copies ou d'extraits par tout procédé; |
| (c) to install, maintain or remove any thing. | **c)** l'installation, l'entretien et l'enlèvement d'objets. |
| **Activities outside Canada** | **Activités à l'extérieur du Canada** |
| (3.1) Without regard to any other law, including that of any foreign state, a judge may, in a warrant issued under subsection (3), authorize activities outside Canada to enable the Service to investigate a threat to the security of Canada. | **(3.1)** Sans égard à toute autre règle de droit, notamment le droit de tout État étranger, le juge peut autoriser l'exercice à l'extérieur du Canada des activités autorisées par le mandat décerné, en vertu du paragraphe (3), pour permettre au Service de faire enquête sur des menaces envers la sécurité du Canada. |
| **Matters to be specified in warrant** | **Contenu du mandat** |
| (4) There shall be specified in a warrant issued under subsection (3) | **(4)** Le mandat décerné en vertu du paragraphe (3) porte les indications suivantes : |
| (a) the type of communication authorized to be intercepted, the type of information, records, documents or things authorized to be obtained and the powers referred to in paragraphs (3)(a) to (c) authorized to be exercised for that purpose; | **a)** les catégories de communications dont l'interception, les catégories d'informations, de documents ou d'objets dont l'acquisition, ou les pouvoirs visés aux alinéas (3)a) à c) dont l'exercice, sont autorisés; |
| (b) the identity of the person, if known, whose communication is to be intercepted or who has possession of the information, record, document or thing to be obtained; | b) l'identité de la personne, si elle est connue, dont les communications sont à intercepter ou qui est en possession des informations, documents ou objets à acquérir; |
| (c) the persons or classes of persons to whom the warrant is directed; | c) les personnes ou catégories de personnes destinataires du mandat; |
| (d) a general description of the place where the warrant may be executed, if a general description of that place can be given; | **d)** si possible, une description générale du lieu où le mandat peut être exécuté; |
| (e) the period for which the warrant is in force; and | e) la durée de validité du mandat; |
| (f) such terms and conditions as the judge considers advisable in the public interest. | f) les conditions que le juge estime indiquées dans l'intérêt public. |

| | |
|---|---|
| **Maximum duration of warrant** | **Durée maximale** |
| (5) A warrant shall not be issued under subsection (3) for a period exceeding | (5) Il ne peut être décerné de mandat en vertu du paragraphe (3) que pour une période maximale : |
| (a) sixty days where the warrant is issued to enable the Service to investigate a threat to the security of Canada within the meaning of paragraph (d) of the definition of that expression in section 2; or | a) de soixante jours, lorsque le mandat est décerné pour permettre au Service de faire enquête sur des menaces envers la sécurité du Canada au sens de l'alinéa d) de la définition de telles menaces contenue à l'article 2; |
| (b) one year in any other case. | b) d'un an, dans tout autre cas. |
| **Application for warrant — measures to reduce threats to the security of Canada** | **Demande de mandat — mesures pour réduire les menaces envers la sécurité du Canada** |
| 21.1 (1) If the Director or any employee who is designated by the Minister for the purpose believes on reasonable grounds that a warrant under this section is required to enable the Service to take measures, within or outside Canada, to reduce a threat to the security of Canada, the Director or employee may, after having obtained the Minister's approval, make an application in accordance with subsection (2) to a judge for a warrant under this section. | 21.1 (1) Le directeur ou un employé désigné à cette fin par le ministre peut, après avoir obtenu l'approbation du ministre, demander à un juge de décerner un mandat en conformité avec le présent article s'il a des motifs raisonnables de croire que le mandat est nécessaire pour permettre au Service de prendre, au Canada ou à l'extérieur du Canada, des mesures pour réduire une menace envers la sécurité du Canada. |
| **Matters to be specified in application** | **Contenu de la demande** |
| (2) An application to a judge under subsection (1) shall be made in writing and be accompanied by the applicant's affidavit deposing to the following matters: | **(2)** La demande est présentée par écrit et accompagnée de l'affidavit du demandeur portant sur les points suivants : |
| (a) the facts relied on to justify the belief on reasonable grounds that a warrant under this section is required to enable the Service to take measures to reduce a threat to the security of Canada; | **a)** les faits sur lesquels le demandeur s'appuie pour avoir des motifs raisonnables de croire que le mandat est nécessaire pour permettre au Service de prendre des mesures pour réduire une menace envers la sécurité du Canada; |
| (b) the measures proposed to be taken; | b) les mesures envisagées; |
| (c) the reasonableness and proportionality, in the circumstances, of the proposed measures, having regard to the nature of the threat, the nature of the measures and the reasonable availability of other means to reduce the threat; | **c)** le fait que les mesures envisagées sont justes et adaptées aux circonstances, compte tenu de la nature de la menace et des mesures, ainsi que des solutions de rechange acceptables pour réduire la menace; |
| (d) the identity of the persons, if known, who | d) l'identité des personnes qui sont touchées |

| | |
|---|---|
| are directly affected by the proposed measures; | directement par les mesures envisagées, si elle est connue; |
| (e) the persons or classes of persons to whom the warrant is proposed to be directed; | e) les personnes ou catégories de personnes destinataires du mandat demandé; |
| (f) a general description of the place where the warrant is proposed to be executed, if a general description of that place can be given; | **f)** si possible, une description générale du lieu où le mandat demandé est à exécuter; |
| (g) the period, not exceeding 60 days or 120 days, as the case may be, for which the warrant is requested to be in force that is applicable by virtue of subsection (6); and | **g)** la durée de validité applicable en vertu du paragraphe (6), de soixante jours ou de cent vingt jours au maximum, selon le cas, demandée pour le mandat; |
| (h) any previous application made under subsection (1) in relation to a person who is identified in the affidavit in accordance with paragraph (d), the date on which each such application was made, the name of the judge to whom it was made and the judge's decision on it. | h) la mention des demandes antérieures présentées au titre du paragraphe (1) touchant des personnes visées à l'alinéa d), la date de chacune de ces demandes, le nom du juge à qui elles ont été présentées et la décision de celui-ci dans chaque cas. |
| **Issuance of warrant** | **Délivrance du mandat** |
| (3) Despite any other law but subject to the Statistics Act, if the judge to whom an application under subsection (1) is made is satisfied of the matters referred to in paragraphs (2)(a) and (c) that are set out in the affidavit accompanying the application, the judge may issue a warrant authorizing the persons to whom it is directed to take the measures specified in it and, for that purpose, | **(3)** Par dérogation à toute autre règle de droit mais sous réserve de la Loi sur la statistique, le juge à qui est présentée la demande visée au paragraphe (1) peut décerner le mandat s'il est convaincu de l'existence des faits qui sont mentionnés aux alinéas (2)a) et c) et énoncés dans l'affidavit qui accompagne la demande; le mandat autorise ses destinataires à prendre les mesures qui y sont indiquées. À cette fin, il peut autoriser aussi, de leur part : |
| (a) to enter any place or open or obtain access to any thing; | a) l'accès à un lieu ou un objet ou l'ouverture d'un objet; |
| **(b)** to search for, remove or return, or examine, take extracts from or make copies of or record in any other manner the information, record, document or thing; | **b)** la recherche, l'enlèvement ou la remise en place de tout document ou objet, leur examen, le prélèvement des informations qui s'y trouvent, ainsi que leur enregistrement et l'établissement de copies ou d'extraits par tout procédé; |
| (c) to install, maintain or remove any thing; or | **c)** l'installation, l'entretien et l'enlèvement d'objets; |
| (d) to do any other thing that is reasonably | **d)** les autres actes nécessaires dans les |

| | |
|---|---|
| necessary to take those measures. | circonstances à la prise des mesures. |
| **Measures taken outside Canada** | **Mesures à l'extérieur du Canada** |
| (4) Without regard to any other law, including that of any foreign state, a judge may, in a warrant issued under subsection (3), authorize the measures specified in it to be taken outside Canada. | **(4)** Sans égard à toute autre règle de droit, notamment le droit de tout État étranger, le juge peut autoriser la prise à l'extérieur du Canada des mesures indiquées dans le mandat décerné en vertu du paragraphe (3). |
| **Matters to be specified in warrant** | **Contenu du mandat** |
| (5) There shall be specified in a warrant issued under subsection (3) | (5) Le mandat décerné en vertu du paragraphe (3) porte les indications suivantes : |
| (a) the measures authorized to be taken; | a) les mesures autorisées; |
| (b) the identity of the persons, if known, who are directly affected by the measures; | b) l'identité des personnes qui sont touchées directement par les mesures, si elle est connue; |
| (c) the persons or classes of persons to whom the warrant is directed; | **c)** les personnes ou catégories de personnes destinataires du mandat; |
| (d) a general description of the place where the warrant may be executed, if a general description of that place can be given; | d) si possible, une description générale du lieu où le mandat peut être exécuté; |
| (e) the period for which the warrant is in force; and | e) la durée de validité du mandat; |
| (f) any terms and conditions that the judge considers advisable in the public interest. | **f)** les conditions que le juge estime indiquées dans l'intérêt public. |
| **Maximum duration of warrant** | **Durée maximale** |
| (6) A warrant shall not be issued under subsection (3) for a period exceeding | **(6)** Il ne peut être décerné de mandat en vertu du paragraphe (3) que pour une période maximale : |
| (a) 60 days if the warrant is issued to enable the Service to take measures to reduce a threat to the security of Canada within the meaning of paragraph (d) of the definition threats to the security of Canada in section 2; or | **a)** de soixante jours, lorsque le mandat est décerné pour permettre au Service de prendre des mesures pour réduire une menace envers la sécurité du Canada au sens de l'alinéa d) de la définition de telles menaces à l'article 2; |
| (b) 120 days in any other case. | **b)** de cent vingt jours, dans tout autre cas. |

B. *Bibliography*

Essential Readings

- **All relevant affidavits, transcripts and submissions**

- **The "McDonald Commission"**
    - [Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *First Report: Security and Information* (Ottawa: Privy Council Office, 1981).]
    - [Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Second Report: Freedom and Security Under the Law*, vol 1-2 (Ottawa: Privy Council Office, 1981).]
    - [Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Third Report: Certain Activities and the Question of Governmental Knowledge* (Ottawa: Privy Council Office, 1981)]
- **The "Pitfield Report"**
    - [Senate of Canada, Special Committee of the Senate on the Canadian Security Intelligence Service, *Delicate Balance: A Security Intelligence Service in a Democratic Society*, (November 1983) (Chair: P.M Pitfield).]
- **The Government's Response to the "Pitfield Report"**
    - [Canada, House of Commons, *The Government's Response to the Report of the Special Committee of the Senate on the Canadian Security Intelligence Service*, (January 1984).]
- **Relevant Hansard Debates**

- [Canada, *House of Common Debates*, 24th Parl, 3rd Sess (10 February 1984) at 1272. Further debates before and after are also useful but are overshadowed by the pertinence of the Minutes of the Standing Committee on Justice and Legal Affairs – see below]

- **Minutes of the Standing Committee on Justice and Legal Affairs discussing the *CSIS Act* in 1984**

  - [House of Commons, *Minutes of Proceedings and Evidence of the Standing Committee on Justice and Legal Affairs*, 32nd Parl, 2nd Sess, No 28 (24 May 1984) at p 28:52 (Chair: Claude-André Lachance).]

- **The Mandatory 5-Year Review Report following the enactment of the *CSIS Act***

  - [Canada, House of Commons, Special Committee on the Review of the *Canadian Security Intelligence Service Act and Security Offences Act, In Flux But Not In Crisis – Report of the Special Committee on the Review of the CSIS Act and Security Offences Act*, (September 1990) (Chair: Blaine Thacker).]

- **The Government's Response to the Mandatory 5-Year Review Report**

  - [Canada, Solicitor General of Canada, *On Course: National Security for the 1990s – The Government's Response to the Report of the House of Commons Special Committee on the Review of the Canadian Security Intelligence Service Act and the Security Offences Act*, (Pierre H. Cadieux – Solicitor General) (February 1991).]

- **The SIRC's 2014-2015 Annual Report**
    - [Canada, Security Intelligence Review Committee, SIRC Annual Report 2014-2015: *Broader Horizons: Preparing the Groundwork for Change in Security Intelligence Review*, (Ottawa: Public Works and Government Services Canada, 2015).]

Supplementary Resources:

- **The "MacKenzie Commission"**
    - [Canada, Privy Council Office, Report of the Royal Commission on Security (Ottawa: Printing and Publishing Supply and Services Canada, 1969).]
- **The "Kellock-Tashereau Commission" also known as the "Gouzenko Affair"**
    - [Canada, Privy Council, *The report of the Royal Commission Appointed under Order in Council P.C. 411 of February 5, 1946 to Investigate the Fact Relating to and the circumstances Surrounding the Communication, by Public Officials and Other Persons in Positions of Trust of Secret and Confidential Information to Agents of a Foreign Power* (Ottawa: 27 June, 1946).]
- **Analysis of the transition from Bill C-157 to Bill C-9 by Donald McDonald**
    - [Canada, Law and Government Division Research Branch, *A Comparison of Bills C-157 and C-9, the Proposed Canadian Security Intelligence Service Act* (Donald MacDonald) (Ottawa: Library of Parliament, January 1984).]

**FEDERAL COURT**

**SOLICITORS OF RECORD**

| | |
|---|---|
| **DOCKET:** | [redacted] |
| **STYLE OF CAUSE:** | IN THE MATTER OF AN APPLICATION BY [redacted] FOR WARRANTS PURSUANT TO SECTIONS 12 AND 21 OF THE CANADIAN SECURITY INTELLIGENCE ACT, R.S.C. 1985, C. C-23 AND IN THE PRESENCE OF THE ATTORNEY GENERAL AND AMICI AND IN THE MATTER OF [redacted] THREAT-RELATED, ACTIVITIES |
| **PLACE OF CLOSED HEARING:** | OTTAWA, ONTARIO |
| **DATE OF CLOSED HEARING:** | FEBRUARY 25 AND 26, 2016<br>MARCH 1, 2016<br>MARCH 31, 2016<br>APRIL 1, 2016<br>MAY 9, 2016 |
| **JUDGMENT AND REASONS:** | NOËL S J. |
| **DATED:** | OCTOBER 4, 2016 |

**APPEARANCES:**

| | |
|---|---|
| Mr. Robert Frater | FOR THE APPLICANT<br>DEPUTY ATTORNEY GENERAL OF CANADA |
| Ms. Katia Bustros | FOR THE APPLICANT<br>DEPUTY ATTORNEY GENERAL OF CANADA |
| Ms. Karla Unger | FOR THE APPLICANT<br>DEPUTY ATTORNEY GENERAL OF CANADA |
| Ms. Anna Walsh | FOR THE APPLICANT<br>DEPUTY ATTORNEY GENERAL OF CANADA |
| Mr. François Dadour | AMICUS CURIAE |

| | |
|---|---|
| Mr. Gordon Cameron | AMICUS CURIAE |

**SOLICITORS OF RECORD:**

| | |
|---|---|
| William F. Pentney<br>Deputy Attorney General of Canada<br>Ottawa, Ontario | FOR THE APPLICANT |
| Poupart, Dadour, Touma & Associates<br>Montréal, Quebec | AMICUS CURIAE |
| Blakes Law Firm<br>Ottawa, Ontario | AMICUS CURIAE |