Federal Court  Cour fédérale

~~**TOP SECRET**~~

**Date: 20231010**

**Docket: CSIS-3-21**

**Citation: 2023 FC 1341**

**Ottawa, Ontario, October 10, 2023**

**PRESENT: THE CHIEF JUSTICE**

**BETWEEN:**

**IN THE MATTER OF AN APPLICATION BY [ ... ] FOR WARRANTS PURSUANT TO SECTIONS 16 AND 21 OF THE *CANADIAN SECURITY INTELLIGENCE SERVICE ACT*, RSC 1985, c C-23**

**AND IN THE MATTER OF [ ... ]**

## REASONS

## I. Introduction

[1] On January 22, 2021, the Attorney General of Canada [**AGC**] provided the Court with a copy of a report issued by the National Security and Intelligence Review Agency [**NSIRA**]. The report concerned a review of disclosures of confidential information about Canadians by the Communications Security Establishment [**CSE**]. More specifically, the report focused upon the disclosure of Canadian identifying information [**CII**]. This included information about Canadians obtained by CSE in the course of assisting the Canadian Security Intelligence Service [**CSIS** or the **Service**] to execute warrants issued by this Court pursuant to sections 16 and 21 of

the *Canadian Security Intelligence Service Act*, RSC 1985, c C-23 [the **CSIS Act**]. These reasons concern only the disclosure of the latter information by CSE.

[2] After making several troublesome findings, NSIRA concluded that "CSE has disclosed information collected pursuant to the Court's warrants in a manner that contradicts key principles previously outlined to the Court by CSIS." It therefore recommended that the AGC "fully inform the [Court] of CSE's practices related to the disclosure of CII and associated practices deriving from warrants issued by the Court, particularly when it pertains to Canadian officials and other sensitive groups described in this report."

[3] In the context of an application for warrants under section 16 [**Section 16 Warrants**] made shortly thereafter, the Court heard evidence regarding the use and disclosure of CII collected pursuant to such warrants, by CSIS and CSE. In brief, that evidence corroborated NSIRA's above-mentioned conclusion. More incomprehensibly, it appears that CSIS was unaware, at least at any senior level, of the manner in which CSE was treating CII that it collected on behalf of CSIS pursuant to the Section 16 Warrants. This was inconsistent with CSIS's prior representation to the Court that CSE "applies the same stringent internal policies and procedures" as CSIS, to the disclosure of CII: see paragraph 38 below [emphasis added].

[4] Fortunately, the evidence provided to the Court demonstrates that, while CSE applied its own, different, standards in considering requests to disclose CII, this generally did not result in the release of CII that would have been kept confidential by CSIS. Although there were a small number of exceptions, they have been remedied or were not material. More importantly, the

Court has been assured that CSE no longer releases CII collected pursuant to the Court's Section 16 Warrants, without the approval of the Director General [**DG**] of CSIS's [ responsible branch ].

[5] In CSIS's capacity as the party seeking *ex parte* warrants authorizing intrusive search powers, CSIS is responsible and accountable for all information collected pursuant to the Court's warrants. To this end, CSIS is duty-bound to be proactive and diligent in ensuring that such information is treated in accordance with (i) the relevant warrant, including the conditions therein; (ii) any representations previously made to the Court; and (iii) the laws of Canada. This remains true when CSIS engages the assistance of third parties, including CSE, in executing the warrants.

[6] Stated differently, CSIS must ensure that such third parties live up to the same standards to which CSIS itself is subject. This includes those pertaining to CII that is incidentally collected pursuant to the Court's warrants. As explained below, CSIS fell short of its responsibilities and the Court's expectations in this regard.

[7] This appears to have been an institutional failing, rather than a failing of any particular individual or individuals. This failing goes to the heart of CSIS's relationship with the Court. It is a matter of institutional trust. It is incumbent upon CSIS to continue its recent efforts to do better.

[8] This failing was exacerbated when CSIS failed to inform the Court of what it had learned from NSIRA, as soon as it became apparent that NSIRA had identified an issue that was material to the Court's exercise of its statutory discretion to grant an application for warrants.

[9] The Court expects CSIS to inform the Court as soon as it becomes aware of any information related to the Court's warrants, about which the Court might reasonably expect to be apprised. This includes information that might reasonably be considered to be material to the basis upon which the Court exercised its discretion to issue previous warrants.

[10] Despite having provided past assurances to the Court in this regard, CSIS has drawn such information to the attention of the Court well after it ought to have done so, on more than one occasion. In the meantime, the Court continued to issue warrants, unaware of important information that was relevant to its consideration of those warrants. Once again, this is a matter of institutional trust.

[11] The Court's expectations are consistent with a commitment given by Mr. Michel Coulombe, the immediate predecessor of CSIS's current Director, regarding issues that might be raised in a review by the Security Intelligence Review Committee – NSIRA's predecessor. Specifically, he committed to advising the Court "as soon as an issue comes up" in a review by the Security Intelligence Review Committee, "even if the report is not finalized": Transcript, *en banc* hearing, June 10, 2016, at 55. The spirit of this commitment was reiterated to me in 2018 by the current Director of CSIS. Fortunately, the Court now appears to be obtaining this type of information on a more timely basis.

## II. Background

[12] NSIRA's review was conducted in 2019 and 2020 under paragraphs 8(1)(a) and (b) of the *National Security and Intelligence Review Agency Act*, SC 2019, c 13, s 2. It was focused on CSE's disclosure of CII. Consequently, NSIRA did not review in detail CSIS's own disclosures of CII obtained pursuant to Section 16 Warrants. Insofar as its review concerned CSIS, it was primarily focused on CSIS's policies, procedures and statistical information, for the purpose of ascertaining whether CSE's disclosures met CSIS's internal standards. Nevertheless, NSIRA noted that, during the period of its review, "CSIS only released two identities outside of the core requesters of [Privy Council Office] and [Global Affairs Canada] to just two other departments": *CSE's Disclosures of Canadian Identifying Information (CII) – (NSIRA Review 08-501-3)* [the **Report]**, at para 105.

[13] The Report was initially scheduled to be completed in the spring of 2020. However, due to the outbreak of the COVID-19 pandemic during the final stages of the review, the completion of the Report was delayed. It was ultimately provided to the Minister of National Defence on November 25, 2020, who in turn provided it to the AGC in January 2021. Shortly thereafter, it was provided to the Court.

[14] The Report has three general areas of focus. The first is upon the legal, policy and operational foundation for CSE's CII disclosure regime, as well as the general parameters of the disclosure process. The second addresses NSIRA's observations, findings and recommendations pertaining to the CII disclosure regime, including CSE's internal practices. The third pertains to

CSE's disclosure of CII in the course of assisting CSIS to execute Section 16 Warrants. Such warrants are generally issued to a CSIS employee in their capacity as the applicant in an *ex parte* proceeding. These reasons will focus solely on the findings and recommendations made in connection with that third area of focus of the Report.

[15] For the present purposes, the most relevant findings addressed in the Report are summarized at paragraphs 9-11 of the Executive Summary. In particular, NSIRA found that:

i. -"[T]he Federal Court is unlikely to be aware of key characteristics of CSE's disclosures of CII obtained pursuant to section 16 of the *CSIS Act* … CSE's disclosures of CII from this program also result in the use of section 16 information for purposes of which the Court is unlikely to be aware, and which merit consideration as part of warrant applications."

ii. -"CSE's treatment and dissemination of [CII] differs substantially from the stringent standards communicated to the Court by CSIS, particularly when the information pertains to Canadian public officials."

iii. -"…CSE has released CII, including information about Canadian officials and other sensitive groups, in a manner that contradicts the procedures communicated to the [Court] in support of warrants obtained by CSIS pursuant to section 16 of the *CSIS Act*."

[16] A brief overview of one aspect of CSE's mandate is necessary to provide context: pursuant to subsection 15(2) of the *Communications Security Establishment Act*, SC 2019, c 13, s 76 [the **CSE Act**], CSE's mandate has five aspects, namely: foreign intelligence, cybersecurity and information assurance, defensive cyber operations, active cyber operations and technical and operational assistance. The discussion below is concerned solely with CSE's disclosure of CII in connection with the latter aspect of its mandate.

[17] CII is particularly significant because CSE is not permitted to direct its activities at Canadians: *CSE Act*, subsection 22(1). In carrying out its technical and operational assistance mandate in connection with CSIS, CSE has the same authority, and is subject to the same limitations, as CSIS: *CSE Act*, subsection 25(1). In turn, in the section 16 context, CSIS is prohibited from collecting information or intelligence relating to the capabilities, intentions or activities of Canadians, except insofar as such information may be incidentally collected through the exercise of warranted powers against non-Canadians: *CSIS Act*, subsection 16(2); *Canadian Security Intelligence Act (Re)*, 2012 FC 1437, at paras 5 and 106. For example, the capture of a communication between a foreign target and a Canadian would be incidental as it relates to the Canadian.

[18] In the Report, CII is defined as follows:

> [CII] is a term that encompasses all information that can be used to identify a Canadian person or entity, in addition to foreign persons physically located within Canada. Identifiers can include everything from full or partial names to birth dates, telephone numbers, Internet Protocol (IP) addresses, e-mail addresses, passport numbers, and physical addresses. It is not necessary for an identifier to be clearly linked to a person's name to constitute

> [CII], as many types of recorded information, numbers, characteristics, and codes could possibly lead to the identification of a Canadian. [Footnotes omitted.]
>
> Report, at para 5.

[19] Upon reviewing the Report, I issued a Direction requiring that evidence be presented regarding the use and disclosure of CII collected pursuant to Section 16 Warrants, by CSIS and third parties such as CSE. Such evidence was to be presented during the next application for Section 16 Warrants. I also requested an explanation of why the Court was not previously informed of the important matters identified by NSIRA in relation to the sharing of information collected pursuant to Section 16 Warrants.

[20] After acknowledging that renewals of Section 16 Warrants would continue to be sought in the interim, my Direction stated that the Court would consider short term renewals pending the determination of the issues identified therein (essentially those raised in the Report and described above). The Direction added that the Court was considering the addition of new conditions to its Section 16 Warrants, and that those warrants would be amended following the Court's review of submissions on the matter, including from *amicus curiae*. Ultimately, Ms. Christine Mainville [the **Amicus**] was appointed for this purpose.[1]

[21] The evidence described above was largely provided in affidavits and hearings in July 2021 and in follow up written responses to undertakings that were provided in October and November 2021. Additional responses were provided at the end of January of this year, in

[1] In February of this year, Ms. Mainville was appointed to the Ontario Court of Justice, effective March 9, 2023.

response to a further Direction dated November 29, 2021, and following several status reports that were provided over the course of 2022. Due to delays associated with the COVID-19 pandemic, final written and oral legal submissions were delayed until March 2022. The AGC then provided Reply submissions in early April 2022. Final oral submissions were made on April 12, 2022.

[22] In the meantime, I granted the requested warrants in March 2021 for a shorter period than would ordinarily be the case, with a new condition [**CII Warrant Condition**][2] and various other changes that are not relevant for the present purposes. The objectives of the new condition are to (i) confirm that any CII retained pursuant to the warrants will be treated pursuant to guidelines issued by the [ Intelligence Assessment Branch [**IAB**] ], entitled *Minimization in IAB Products*, and (ii) require any requested "unminimization" to be approved by the **DG** [ of the responsible branch ]. Given the delays described above, I extended the warrants.

[23] During one of the hearings in this proceeding, the Amicus adduced a copy of an unclassified version of a document entitled *CSE Management Response to NSIRA Review of 2018-2019 Disclosures of Canadian Identifying Information*, dated May 31, 2021. Among other things, CSE observed in that document that it was "concerned that the overall conclusions [in the Report] do not fully appreciate CSE's commitment to, and work on protection of privacy." CSE also noted that its "case-by-case process for disclosing CII to authorized [Government of

[2] This condition is discussed further below.

Canada] recipients is part of robust and comprehensive internal measures that protect Canadians' privacy." Those measures were described as follows:

> The obfuscation of this [CII] in reporting represents one of many layered privacy measures that are applied at different points in CSE's end-to-end intelligence process. These include, among others, legal and policy training and on-site support for intelligence analysts, mandatory annual privacy tests for all operational employees, data tagging and auto-deletion, strict retention limits, specific handling guidelines, escalating approvals for reporting that includes Cll, compliance spot checks, and separate vetting processes for disclosing obfuscated information and taking action on intelligence reporting.

[24] On May 31, 2022, the AGC informed the Court of instances of non-compliance with the CII Warrant Condition and the related commitment of CSIS to conduct a review of CII disclosure and to inform the Court of its outcome and the corrective measures implemented. After providing several status reports over the course of 2022 regarding that review, the AGC provided an affidavit affirmed by [ the affiant ], DG [ of the responsible branch ], dated January 31, 2023.

[25] In that affidavit, [ the affiant ] explained that the abovementioned review pertained to all CSIS Intelligence Reports [**CIRs**] issued by CSIS pursuant to section 16 of the *CSIS Act* between April 1, 2021 and June 30, 2022. Ultimately, that review identified 159 instances of non-compliance with the CII Warrant Condition. In each case, such non-compliance resulted in the unminimization of CII without the approval of the DG [ of the responsible branch ], as required by the CII Warrant Condition. [ The affiant ] attributed those instances of non-compliance to internal miscommunication of the CII Warrant Condition, as well as a misunderstanding of that condition and a lack of technology to enforce approval levels. After reviewing each of those

instances of non-compliance, [ the affiant ] confirmed that he would have authorized disclosure for one or more of the reasons stipulated in the CII Warrant Condition.

[26] [ The affiant ] further explained that a similar review was conducted for section 16 reports issued by CSE, also known as End-Product Reports [**EPRs**]. That review identified [ ... ] further instances of non-compliance with the CII Warrant Condition. Once again, [ the affiant ] confirmed that he would have authorized disclosure in all instances, for one or more of the reasons stipulated in the CII Warrant Condition.

[27] Finally, after identifying various possible causes for the above-described non-compliance, [ the affiant ] assured the Court that corrective measures are now in place to address those shortcomings, and that additional corrective measures may be implemented following further review.

## III. Section 16 of the CSIS Act

[28] Section 16 authorizes CSIS to collect, within Canada, information or intelligence relating to the capabilities, intentions or activities of any foreign state, group of foreign states, or any person other than a Canadian citizen, permanent resident or corporation incorporated by or under Canadian federal or provincial law. This collection must be for the purposes of assisting the Minister of National Defence or the Minister of Foreign Affairs in relation to the defence of Canada or the conduct of international affairs in Canada.

[29] An important precondition to the exercise of the authority conferred by section 16 is that either the Minister of Foreign Affairs or the Minister of National Defence must personally request CSIS's assistance. The Court understands that most requests are made by the Minister of Foreign Affairs. In any event, the Court understands that these Ministerial requests are generally made by way of a Letter of Request and an accompanying annex – referred to as the "Rationale" for the request. That Rationale generally sets out the specific intelligence requirements of the requesting Minister, under the heading "Clear Requirements/Tasking." These requirements are strategic in nature and describe the areas and matters of interest to the particular Minister in their defence of Canada or their conduct of the international affairs of Canada.

[30] A second precondition to the exercise of the authority described above is that the Minister of Public Safety and Emergency Preparedness personally consents thereto, in writing.

[31] Both of the aforementioned preconditions were satisfied in the present proceeding.

[32] The full text of section 16 is set forth in Appendix 1 hereto.

## IV. Observations and Findings

[33] I will now turn to the three findings of NSIRA reproduced at paragraph 15 above.

### A. *The Court's Unawareness of Key Characteristics of CSE's Disclosure of CII and of the Scope of Those Disclosures*

#### (1) What the Court understood prior to this proceeding

[34] The Court has had extensive exchanges over many years with CSIS and the AGC regarding the collection and retention of incidentally collected information relating to Canadians. Many of these exchanges have concerned the potential uses and disclosures of CII.

[35] The process of obfuscating CII is referred to as "minimization" within CSIS and "suppression" within CSE.

[36] Prior to reviewing the Report, the Court's understanding of CSE's disclosures of CII was based on the affidavit evidence addressed at paragraphs 90-93 of the Report. That evidence was adduced in a Section 16 proceeding in 2013-2014. During that proceeding, the Court requested:

> …a step by step detailed account of how and by whom [CSIS's Minimization Policy] is applied at CSIS and at the [CSE] including the factors considered on each occasion when CSIS or the CSE decides whether the disclosure of a Canadian's identity is necessary to understand or exploit the intelligence.

[37] Through two affidavits sworn in that proceeding by [ a CSIS affiant ], the Court was provided with a brief description of, among other things:

i. CSIS's control over the dissemination of intelligence reports drafted by CSE;

ii. the caveats upon the uses that may be made of such reports, or of information contained therein, by recipients;

iii. CSE's processing and treatment of the "raw material" obtained pursuant to Section 16 Warrants;

iv. CSIS's policy regarding the "minimization" of CII in intelligence reports, and the implementation of that policy within CSIS and CSE; and

v. how CSIS and CSE deal with requests by those recipients for the disclosure of a Canadian's identity, also known as "unminimization."

[38] The information provided by [ the CSIS affiant ] in relation to the treatment of CII was significantly less detailed for CSE than it was for CSIS. Nevertheless, the Court was assured that CSE "applies the same stringent internal policies and procedures to protect Canadian identities derived from section 16 information in conformity with Condition 1 of the warrants": Affidavit of [[ the CSIS affiant ] **Affidavit #1]** [emphasis added]. The Court understands the words "the same" to refer to CSIS's internal policies and procedures.

[39] The Court's understanding that CSIS exercised control over the dissemination of CII by CSE was also based on the following two passages of affidavit evidence provided by [ the CSIS affiant ]:

> i. 15. When CSE agrees to act as an agent of the service, it is acting under the Service's authority and abides by the conditions of the warrants granted under sections 16 and 21 of the [*CSIS Act*]. Both the Service and CSE ensure compliance with the terms of the warrants and process the raw material collected through the execution of the warrants.

> 16. Processing raw material means [ developing tools and techniques, intercepting target communications, decryption, report writing and translation ]. In the case of CSE-debriefed material, the Service must authorize the dissemination of the reports. This step is meant to ensure consistency and compliance with the warrant conditions and Service policy.
>
> [ CSIS affiant ] Affidavit #1, emphasis added

ii. 26. This limited readership [of CSIS and CSE intelligence reports], as compared to the overall employee population of government departments and agencies, demonstrates both the high level of security attached to CSIS external reports and the subsequent care the Service takes in limiting the unnecessary propagation of sensitive national security information. Coupled with the Service's and CSE's minimization of Canadian identities, I believe that the Service has taken and continues to take the necessary steps to protect the privacy of Canadians.

[[ CSIS affiant ] **Affidavit #2]** [emphasis added].

[40] Additional evidence that was provided regarding the caveats imposed at the time intelligence reports are disseminated supports the Court's prior understanding regarding CSIS's control. In this regard, [ the CSIS affiant ] stated that "[a]ll external reports are accompanied by caveats that require the clients to seek the Service's permission to make any further use of [foreign intelligence] reports or of information contained therein": [ CSIS affiant ] Affidavit #1, at para 31 [emphasis added].

[41] Turning to CSIS's strict approach to the "minimization" of CII in intelligence reports, [ the CSIS affiant ] evidence was consistent with evidence provided by his successor in 2017. That evidence is summarized in *Canadian Security Intelligence Service Act (Re)*, 2020 FC 697,

at paras 33 to 42 [***Re X (2020)***]. It is unnecessary to repeat it here. For the present purposes, it will suffice to note that the evidence filed in that proceeding made only passing references to the disclosure of CII by CSE. This is despite the fact that, in the Direction leading to that proceeding, the Court specifically requested that it be provided with a better understanding of "the retention practices regarding intercepted communications following collection pursuant to section 16 warrants involving Canadians": Direction of Justice Simon Noël, June 20, 2017, CSIS-9-17.

[42] Regarding the specific manner in which CSE deals with requests to disclose (i.e., "unminimize" or "unsuppress") a Canadian's identity, the evidence received by the Court prior to this proceeding appears to have been limited to the following statement:

> [ A senior CSE official is the authority for releasing privacy-sensitive information minimized from foreign intelligence. To streamline the process and CSE's support to government departments and agencies, this official has delegated the authority to a specific unit that validates and releases suppressed information ].
>
> [ CSIS affiant ] Affidavit #2, at para 20.

[43] Given the evidence discussed at paragraphs 37-40 above, the Court did not understand that the statement quoted immediately above might apply to CII collected pursuant to Section 16 Warrants.

[44] The Court's understanding that CSIS exercised control over the dissemination of all CII collected pursuant to Section 16 Warrants is consistent with the evidence of CSIS's affiant in the present proceeding. Specifically, [ a CSIS witness ], DG [ of the responsible branch ] at that

time, testified that CSIS did not believe that CSE had the authority to disclose CII collected pursuant to Section 16 Warrants, on its own: Transcript, July 22, 2021, at 138; see also 49-50.

[45] In a similar vein, the AGC's written submissions in this proceeding state: "[t]he [AGC] was not aware, before the NSIRA review, that CSIS and CSE followed their own separate policies and practices regarding the disclosure of CII and acknowledges that the Court should have been specifically advised."

(2) Important aspects of CSE's approach to CII of which the Court was unaware

[46] The Report identified several differences in the manner in which CSIS and CSE, respectively, treat CII collected pursuant to Section 16 Warrants. These were summarized at Annex D to the Report, which is reproduced immediately below. (Footnotes and an example of an external report approval and dissemination have not been reproduced.)

| Issue | CSIS | CSE |
|---|---|---|
| Publication and readership of s. 16 external intelligence reports | Distributed only to those individuals with a need-to-know.<br>Largely PCO and GAC | Distributed to all Canadian readership through SLINGSHOT<br>At least seven departments other than PCO and GAC |
| Approval of sensitive reports detailing activities of foreign states specific to Canadian officials | Approval from Director or his/her designate (e.g. Assistant Director) required to externally report | Approval by CSIS operational desk (Analyst or Head) |
| Minimization procedures for s. 16 collected CII | Service employees following CSIS procedures | CSE employees following CSE's procedures |
| Approach to minimization | Authorized readers of external reports do not generally need to know the identity of Canadians | No specific approach, but all 107 s. 16 identities in review period were released |
| Disclosure of CII generally | CSIS [ responsible branch ] receives request, forwards it | CSE receives request and approves without specific |

| | | |
|---|---|---|
| | to the relevant operational branch for consideration | knowledge that report originates from assistance to CSIS |
| Disclosure practices/requirements | No specific guidelines, refers to its minimization policy | Clients must have a lawful authority and an operational justification |
| Disclosures pertaining to Canadian officials | Generally approved at ADI/management level | Generally approved at the CSE analyst level |
| Compliance with warrant conditions and limitations of s. 16 | Governance structure instituted, with access to information tightly controlled and compartmentalized | Follows its own policies for disclosure of CII and compliance with warrant conditions, independent of any policies at CSIS |

[47] Prior to reviewing the Report, the Court was not aware of CSE's practices in respect of the foregoing aspects of its treatment of CII. The Court also did not appreciate that CII collected pursuant to Section 16 Warrants might be disseminated to a much broader range of potential recipients than it had previously understood.

[48] The above-mentioned differences regarding the treatment of CII by CSIS and CSE, respectively, are such that I agree with NSIRA's finding that "CSE has released CII, including information about Canadian officials and other sensitive groups, in a manner that contradicts the procedures communicated to the [Court] in support of warrants obtained by CSIS pursuant to section 16 of the *CSIS Act*": Report, Executive Summary, at para 11.

[49] I also agree with NSIRA's intimation that, had the Court been aware that CSE had its own CII disclosure regime, the Court would have required CSE to take steps similar to those that had been adopted by CSIS in this regard: Report, at paras 99-101. In particular, I share NSIRA's view that the Court would have required CSE to develop guidelines for distributing and

unminimizing CII, and to provide the Court with an opportunity to comment on those guidelines prior to their finalization: Report, at paras 98-101.

(3) Ownership of CII Collected Pursuant to Section 16 Warrants

[50] The Report identified an important issue regarding the "ownership" of CII obtained pursuant to Section 16 Warrants. Specifically, at footnote 125, the Report refers to a 2014 CSIS document entitled *DDO Directive on Section 16 of the CSIS Act* **[**the **2014 DDO Directive]**, which stated that once an "End-Product Report" drafted by CSE has been approved by CSIS, "it – and the information it contains – effectively belongs to CSE": 2014 DDO Directive, at p 12.

[51] While that Directive was before the Court in ***Re X (2020)***, its significance in relation to the ownership of the information and what that meant with respect to the disclosure of CII by CSE was not brought to the Court's attention. Consequently, the Court continued to understand that CSIS remained in control of all CII collected pursuant to Section 16 Warrants. This is reflected in the only references to the Directive in ***Re X (2020)***, which did not address the ownership and control of CII: ***Re X (2020)***, at paras 30 and 34.

[52] NSIRA interpreted this passage from the DDO 2014 Directive as suggesting that CSIS "releases ownership of s. 16-collected information to CSE when it approves CSE's reports prepared under assistance": Report, at para 91. However, this understanding was rejected by the senior representatives of CSIS and CSE who testified during the present proceeding. Specifically, [ the CSIS witness ], on behalf of CSIS, stated that the above-quoted passage from the DDO 2014 Directive "is not correct" because "the Service still owns, in reality, the

information": Transcript, July 22, 2021, at 118-119. Likewise, when asked whether CSE takes ownership over information collected pursuant to Section 16 Warrants, [ ... ], CSE's Deputy Chief of Policy and Communications, stated as follows:

> I would say no. [ ... ], we still consider that to be CSIS information. That's why they release a report, not us. All of that is CSIS information, in accordance with CSE policy, as well.
>
> Transcript, July 28, 2021, at 31.

[53] The testimony of [ the CSIS witness ] and [ the CSE witness ] on this point is consistent with the AGC's position, which is that "CSE has never had control over CII when that information was collected by CSIS." The sole exception is where CII may ultimately be disclosed to CSE to fulfil another aspect of its mandate under section 15 of the *CSE Act*, such as its foreign intelligence mandate. In written submissions, the AGC elaborated as follows:

> 96. Disclosure of s. 16 CII is a different process. Although CSE facilitates the disclosure of supressed CII as part of its assistance mandate, and despite conflicting statements in the past, it is undisputed that CSE acts as custodian over information in the s. 16 process and has no ownership of that information.

[54] This confirmation of CSIS's ownership of CII collected pursuant to Section 16 Warrants is consistent with the following statement that appears at paragraph 4.1.1 of CSIS's OPS-221 policy, entitled *Processing of Information and Communications Collected under Warrant – Section 16*, (2014-07-03): "[f]oreign intelligence processed by CSE on behalf of the Service remains under Service control until authorized for disclosure to the requesting Minister or designate by the Chief, CSE Liaison Section or designate."

[55] In 2018, Mr. Dominic Rochon, CSE's Deputy Chief, Policy and Communications, made a similar statement to House of Commons Standing Committee on Public Safety and National Security. Specifically, he stated:

> Today, as with this new legislation, if CSIS is interested in you, they have to have a legal mandate to go after you, meaning they have to get a warrant. If they show us that they have a warrant, at that point in time they wouldn't have access to our systems. They would ask us to act on their behalf. We would then use our capabilities to help them collect information. Any information that we collect is segregated and is given back to them and is their information. Effectively, we are acting on behalf of CSIS.
>
> House of Commons, Standing Committee on Public Safety and National Security, 42nd Parliament, 1st Session, Thursday, March 22, 2018, at 17 [emphasis added].

[56] Having regard to all of the foregoing, I am satisfied that CSIS retains ownership of CII collected pursuant to its warrants, and that any past statements that may have suggested otherwise were not correct.

B. *CSE's Treatment and Dissemination of CII Differed Substantially from the Stringent Standards Communicated to the Court by CSIS*

[57] The evidence in this proceeding substantiates NSIRA's finding that "CSE's treatment and dissemination of [CII] differs substantially from the stringent standards communicated to the Court by CSIS, particularly when the information pertains to Canadian public officials": Report, at para 9.

[58] The Court's prior understanding of CSIS' policies and practices with respect to CII are summarized in *Re X (2020)*, at paras 33-42. In that decision, the Court characterized those

policies and practices as being "generally adequate and consonant with [CSIS's] s 16 mandate": *Re X (2020),* at para 51. Nevertheless, the Court agreed with the *amici* that CSIS "should develop criteria and guidelines on the unminimization of identifying information about Canadians": *Re X (2020)*, at para 51; see also para 74.

[59] Through the current proceeding, the Court's understanding of CSIS's policies and practices with respect to CII has been supplemented. Most significantly, [ the CSIS witness ] testified that CSIS is also guided by *IAB Guidelines: IAB-GO1, Minimization in IAB Products*, which were updated in December 2020. [ The CSIS witness ] added that CSIS was in the process of finalizing a new procedure governing minimization, entitled *Minimization and Un-Minimization of Canadian Identifying Information (CII) in IAB S.16 Products*. In November 2021, the Court was provided with the final version of that document [the **New CSIS CII Policy**].

[60] It is unnecessary to go through the New CSIS CII Policy in detail. For the present purposes, it will suffice to note that it was drafted partially in response to NSIRA's recommendations and partially in response to issues raised during the present proceeding. It is noteworthy that the document observed that both NSIRA and this Court "have acknowledged that the legal authority for s. 16 reporting stems exclusively from the *CSIS Act* and that the Service is responsible for its application, and responds directly to the [Court] in this regard": New CSIS CII Policy, at para 1.3.

[61] The New CSIS CII Policy includes new sections devoted to "Responsibilities" (section 2) and "Notification & Consultation Requirements" (section 5). In keeping with the new CII Condition that has been added to the Court's warrants, and consistent with the representations made to during the hearing, the New CSIS CII Policy makes it clear that "[_the responsible branch_ is the Program Owner of all matters related to this procedure, including: guidance, implementation, monitoring and review": New CSIS CII Policy, at para 1.10. Further, it is stipulated that "[t]he DG [_of the responsible branch_] is responsible for ensuring that all individuals/agencies addressing [Section 16] minimization procedures are familiar, and compliant, with this procedure…": New CSIS CII Policy, at para 2.1. Finally, paragraph 5.1 includes the following "notification and consultation" provision:

> In cases of non-compliance with the above-noted procedure, CSIS and/or any relevant OGD responding to CSIS' s.16 [Requests for Assistance] , and the [AGC] will inform the [Court] in accordance with the warrant conditions of CSIS' and/or the OGD's actions related the disclosure of CII and associated practices deriving from warrants issued by the Court, particularly as they pertain [_ to Canadian public officials and other sensitive groups _].

[62] Considering the foregoing, CSIS's current policies and practices in relation to CII do not warrant further comment at this time.

[63] The most noteworthy differences in the manner in which CSIS and CSE, respectively, treated CII collected pursuant to Section 16 Warrants were summarized at Annex D to the Report. That Annex is reproduced at paragraph 46 above. The evidence in this proceeding largely substantiates NSIRA's understanding of those differences in the treatment of such CII by CSIS and CSE, respectively, prior to NSIRA's review. Given the important changes that CSE

has made to its policies and practices, it is unnecessary to further comment upon those past differences.

[64] Most significantly, as a result of NSIRA's findings, CSE implemented changes that include modifying the level of authority for approving requests for disclosure of suppressed CII, including requests pertaining to section 16 reporting. Beginning January 11, 2021, requests for disclosure of suppressed CII were reviewed by a Disclosure Analyst and approved by a Supervisor. Shortly afterwards, on February 15, 2021, responsibility for assessing and approving such requests was transferred, at CSIS's request, to the DG [ of the responsible branch ]. However, CSE continued to assess and approve requests from CSIS until April 30, 2021, at which time CSIS clarified that all requests for disclosure of suppressed CII, including those from CSIS, must be sent to the DG [ of the responsible branch ] for assessment and approval.

[65] Consequently, CSE no longer assesses and approves requests for disclosure of suppressed CII contained in section 16 reporting. Such requests are still sent through CSE's web-based tool. However, CSE now forwards such requests to the DG [ of the responsible branch ]. If and when the DG [ of the responsible branch ] approves unminimization of CII, that information is provided to the requesting agency. I understand that this accounts for the technical realities that [ ... ].

## V. New Warrant Condition

[66] The CII Warrant Condition discussed at paragraph 22 above, and included in the Court's warrants since March 31, 2021, provides as follows:

> Any information about Canadians, retained in accordance with Condition 1, that would identify a Canadian shall not be disclosed by the Service or the Communications Security Establishment unless the information
>
> (a) is necessary to the understanding or exploitation of the foreign intelligence;
>
> (b) concerns activities which there are reasonable ground to believe constitute a threat to the security of Canada as defined in section 2 of the [CSIS] *Act*;
>
> (c) concerns the prevention, investigation or prosecution of an alleged indictable offence; or
>
> (d) is already available in the public domain
>
> and is approved for disclosure by the Director General, [ of the responsible branch ] of the Service or her designate.

[67] Given the Court's understanding of CSIS's practices, procedures **[and guidelines]** with respect to CII, the Court is satisfied that the terms of the CII Warrant Condition are sufficient at this time.

## VI. CSIS's Duty of Candour

[68] In recent years, the Court has had extensive exchanges with CSIS and the AGC regarding CSIS's duty of candour in *ex parte* proceedings. Some of those exchanges were discussed in *Canadian Security Intelligence Services Act (Re)*, 2020 FC 616, at paras 83-85, 91-100 and 167. It is unnecessary to repeat them here.

[69] For the present purposes it will suffice to note that this duty was triggered as soon as CSIS became aware that CSE was disclosing CII pursuant to its own, materially different, policies and practices.

[70] [ The CSIS witness ] repeatedly testified that, prior to reviewing the Report, CSIS was not aware that CSE was receiving requests to "unminimize" obfuscated CII in intelligence reports that it had distributed, after receiving authorization to do so from CSIS: Transcript, July 22, 2021, at 28, 39, 47, 49-50 and 74. She described this as a "miscommunication": Transcript, July 22, 2021, at 47.

[71] This evidence is not entirely consistent with testimony provided by [ the CSE witness ]. After stating that he did not know what CSIS was aware of, he explained that he "understood" that "at least a portion of CSIS" was aware that CSE was disclosing CII obtained pursuant to Section 16 Warrants: Transcript, July 28, at 15 and 58. However, he did not identify who within CSIS may have been so aware.

[72] [ The CSIS witness ] testimony is corroborated by the AGC. As previously mentioned, the Court was informed in written submissions that the AGC "was not aware, before the NSIRA review, that CSIS and CSE followed their own separate policies and practices regarding the disclosure of CII and acknowledges that the court should have been specifically advised."

[73] I find it very surprising, to say the very least, that CSIS was not aware that CSE was "unminimizing"/"unsuppressing" CII obtained pursuant to Section 16 warrants, and doing so

further to its own, materially different, policies and practices. However, I am prepared to accept the evidence of [ the CSIS witness ] and the assurances of the AGC in this regard.

[74] In any event, CSIS still had an obligation to inform the Court about what it had learned regarding CSE's disclosures, as soon as it became aware of them. In my view, this must have been well in advance of January 22, 2021, when the AGC provided a copy of the Report to the Court.

[75] According to a list of meetings and briefings set forth in Annex G to the Report, NSIRA met with CSIS on December 2, 2019, after receiving seven separate briefings from CSE in the preceding months. I find it very difficult to believe that CSIS did not obtain a good sense, either at that time or in the ensuing months, of the nature of NSIRA's concerns in relation to CSE's unminimizing of CII pursuant to its own, materially different, disclosure regime. Whenever that initial understanding of CSE's practices in this regard was obtained, CSIS's duty of candour to the Court crystallized.

[76] Particularly given that the Court was continuing to grant Section 16 Warrants, CSIS could not wait until NSIRA's report had been finalized or was close to being final. Nor could CSIS wait until it had a complete understanding of the nature of NSIRA's concerns, or of the full extent of CSE's policies and practices.

[77] CSIS should have informed the Court of what it had learned as soon as it became aware that CII obtained pursuant to Section 16 Warrants was being unminimized and disseminated by

CSE without CSIS's knowledge and pursuant to policies and practices that might be different from the CSIS policies and practices previously communicated to the Court. Quite apart from the fact that the Court was continuing to grant Section 16 Warrants, this information might well have led the Court to revisit previously issued warrants, depending on the nature of that information.

[78] Beyond all of the foregoing, in 2016, CSIS's Director made a commitment to the Court to advise the Court "as soon as an issue comes up" in a review by the Security Intelligence Review Committee (NSIRA's predecessor), "even if the report is not finalized": Transcript, *en banc* hearing, June 10, 2016, at 55. This was on the understanding that the final report and recommendations might be different from what might have been communicated to the Court. The spirit of this commitment was reiterated to me in 2018 by the current Director of CSIS. By waiting until January 22nd of 2021, CSIS fell short of both this commitment and its duty of candour.

[79] Regrettably, this has now happened on more than one occasion since the above-mentioned commitment was initially made in 2016. Fortunately, the Court now appears to be obtaining this type of information on a more timely basis.

## VII. Conclusion

[80] The evidence adduced in this proceeding corroborates NSIRA's finding that CSE disclosed CII collected pursuant to the Court's Section 16 Warrants in a manner that contradicts key principles previously outlined to the Court by CSIS. That evidence also demonstrates that CSIS was unaware, at least at any senior level, of the manner in which CSE was treating such

information. This was inconsistent with CSIS's prior representation to the Court that CSE "applies the same stringent internal policies and procedures" as CSIS, to the disclosure of CII: see paragraph 38 above [emphasis added]. CSE did not apply those same, stringent, standards. Its policies and practices led to the disclosure of CII that would not have met CSIS's internal policies and procedures.

[81] Fortunately, the evidence also demonstrates that while CSE applied its own, different, standards in considering requests to disclose CII, this generally did not result in the release of CII that would have been kept confidential by CSIS. Although there were a small number of exceptions, they have been remedied or were not material. More importantly, the Court has been assured that CSE no longer releases CII collected pursuant to the Court's Section 16 Warrants, without the approval of the DG of [ the responsible branch ]. In addition, the New CSIS CII Policy has led to changes in the manner in which CSIS itself treats CII. Based on the evidence adduced in this proceeding, the Court has no reason at this time to question the manner in which CSIS treats CII obtained pursuant to its Section 16 Warrants.

[82] It bears underscoring that, in CSIS's capacity as the party seeking *ex parte* warrants authorizing intrusive search powers, CSIS is responsible and accountable for all information collected pursuant to the Court's warrants. To this end, CSIS is duty-bound to be proactive and diligent in ensuring that such information is treated in accordance with (i) the relevant warrant, including the conditions therein; (ii) any representations previously made to the Court; and (iii) the laws of Canada. This remains true when CSIS engages the assistance of third parties, including CSE, in executing the warrants.

[83] CSIS's failure to live up to its obligations in this regard appears to have been an institutional failing, rather than a failing of any particular individual or individuals. This failing goes to the heart of CSIS's relationship with the Court. It is a matter of institutional trust. It is incumbent upon CSIS to continue its recent efforts to do better.

[84] This failing was exacerbated when CSIS failed to inform the Court of what it had learned from NSIRA, as soon as it became apparent that NSIRA had identified an issue that was material to the Court's exercise of its statutory discretion to grant an application for warrants.

[85] The Court expects to inform the Court as soon as it becomes aware of any information related to the Court's warrants, about which the Court might reasonably expect to be apprised. This includes information that might reasonably be considered to be material to the basis upon which the Court exercised its discretion to issue previous warrants.

"Paul S. Crampton"

Chief Justice

## Appendix I – Relevant Provisions

*Canadian Security Intelligence Service Act*, RSC, 1985, c C-23.
*Loi sur le Service canadien du renseignement de sécurité*, LRC 1985, c C-23.

| DUTIES AND FUNCTIONS OF SERVICE | FONCTIONS DU SERVICE |
|---|---|
| **16**. (1) Subject to this section, the Service may, in relation to the defence of Canada or the conduct of the international affairs of Canada, assist the Minister of National Defence or the Minister of Foreign Affairs, within Canada, in the collection of information or intelligence relating to the capabilities, intentions or activities of | **16**. (1) Sous réserve des autres dispositions du présent article, le Service peut, dans les domaines de la défense et de la conduite des affaires internationales du Canada, prêter son assistance au ministre de la Défense nationale ou au ministre des Affaires étrangères, dans les limites du Canada, à la collecte d'informations ou de renseignements sur les moyens, les intentions ou les activités : |
| (*a*) any foreign state or group of foreign states; or | *a*) d'un État étranger ou d'un groupe d'États étrangers; |
| (*b*) any person other than | *b*) d'une personne qui n'appartient à aucune des catégories suivantes : |
| (i) a Canadian citizen, | (i) les citoyens canadiens, |
| (ii) a permanent resident within the meaning of subsection 2(1) of the *Immigration and Refugee Protection Act*, or | (ii) les résidents permanents au sens du paragraphe 2(1) de la *Loi sur l'immigration et la protection des réfugiés*, |
| (iii) a corporation incorporated by or under an Act of Parliament or of the | (iii) les personnes morales constituées sous le régime d'une loi fédérale ou provinciale. |

legislature of a province.

(2) The assistance provided pursuant to subsection (1) shall not be directed at any person referred to in subparagraph (1)(*b*)(i), (ii) or (iii).

(3) The Service shall not perform its duties and functions under subsection (1) unless it does so

(*a*) on the personal request in writing of the Minister of National Defence or the Minister of Foreign Affairs; and

(*b*) with the personal consent in writing of the Minister.

…

(2) L'assistance autorisée au paragraphe (1) est subordonnée au fait qu'elle ne vise pas des personnes mentionnées à l'alinéa (1)*b*).

(3) L'exercice par le Service des fonctions visées au paragraphe (1) est subordonné :

*a*) à une demande personnelle écrite du ministre de la Défense nationale ou du ministre des Affaires étrangères;

*b*) au consentement personnel écrit du ministre.

[…]

*Communications Security Establishment Act*, SC, 2019, c 13, s 76.
*Loi sur le Service canadien du renseignement de sécurité*, LC 2019, ch 13, art 76.

MANDATE

**15**. (1)

…

(2) The Establishment's mandate has five aspects: foreign intelligence, cybersecurity and information assurance, defensive cyber operations, active cyber operations and technical and operational assistance.

MANDAT

**15**. (1)

[…]

(2) Le mandat du Centre comporte cinq volets : le renseignement étranger, la cybersécurité et l'assurance de l'information, les cyberopérations défensives, les cyberopérations actives et

l'assistance technique et opérationnelle.

ACTIVITIES

**22.** (1) Activities carried out by the Establishment in furtherance of the foreign intelligence, cybersecurity and information assurance, defensive cyber operations or active cyber operations aspects of its mandate must not be directed at a Canadian or at any person in Canada and must not infringe the Canadian Charter of Rights and Freedoms.

…

**25** (1) If the Establishment provides assistance in furtherance of the technical and operational assistance aspect of its mandate, then the Establishment, in the course of providing the assistance, has the same authority to carry out any activity as would have the federal law enforcement or security agency, the Canadian Forces or the Department of National Defence, as the case may be, if it were carrying out the activity, and is subject to any limitations imposed by law on the agency, the Canadian Forces or that Department, including requirements with respect to any applicable warrant.

…

ACTIVITÉS

**22.** (1) Les activités menées par le Centre dans la réalisation des volets de son mandat touchant le renseignement étranger, la cybersécurité et l'assurance de l'information, les cyberopérations défensives ou les cyberopérations actives ne peuvent viser des Canadiens ou des personnes se trouvant au Canada et ne peuvent porter atteinte à la Charte canadienne des droits et libertés

[…]

**25** (1) Lorsque, dans la réalisation du volet de son mandat touchant ce domaine, le Centre fournit une assistance technique et opérationnelle à un organisme fédéral chargé de l'application de la loi ou de la sécurité, aux Forces canadiennes ou au ministère de la Défense nationale, le Centre a, quant à l'exercice d'une activité, les mêmes pouvoirs qu'aurait l'organisme fédéral, les Forces canadiennes ou le ministère s'ils menaient cette activité et est assujetti aux limites que la loi leur impose, y compris aux exigences de tout mandat applicable.

[…]

**FEDERAL COURT**

**SOLICITORS OF RECORD**

| | |
|---|---|
| **DOCKET:** | CSIS-3-21 |
| **STYLE OF CAUSE:** | IN THE MATTER OF AN APPLICATION BY [ ... ] FOR WARRANTS PURSUANT TO SECTIONS 16 AND 21 OF THE *CANADIAN SECURITY INTELLIGENCE SERVICE ACT*, RSC 1985, c C-23<br><br>AND IN THE MATTER OF [ ... ] |
| **PLACE OF HEARING:** | OTTAWA, ONTARIO |
| **LAST SUBMISSION OF EVIDENCE** | JANUARY 31, 2023 |
| **DATES OF HEARING:** | MARCH 31, 2021<br>JULY 22 & 28, 2021<br>APRIL 12, 2022 |
| **REASONS:** | CRAMPTON C.J. |
| **DATED:** | OCTOBER 10, 2023 |

**APPEARANCES:**

| | |
|---|---|
| Nancie Couture<br>Christopher Rupar | FOR THE APPLICANT<br>THE ATTORNEY GENERAL OF CANADA |
| Christine Mainville | *AMICUS CURIAE* |

**SOLICITORS OF RECORD:**

| | |
|---|---|
| Attorney General of Canada<br>Ottawa, Ontario | FOR THE APPLICANT |
| Henein Hutchison Robitaille LLP<br>Toronto, Ontario | *AMICUS CURIAE* |