Federal Court  Cour fédérale

~~**TOP SECRET**~~

Date: 20221021

Docket: CSIS-1-21

Citation: 2022 FC 1444

Ottawa, Ontario, October 21, 2022

PRESENT: THE CHIEF JUSTICE

BETWEEN:

IN THE MATTER OF AN APPLICATION BY [...] FOR WARRANTS PURSUANT TO SECTIONS 12 AND 21 OF THE *CANADIAN SECURITY INTELLIGENCE SERVICE ACT*, RSC 1985, c C-23

AND IN THE MATTER OF [...] THREAT-RELATED ACTIVITIES

JUDGMENT AND REASONS

I. Introduction

[1] As the art of tradecraft for clandestine domestic and international activities continues to evolve, the public interest requires the Canadian Security Intelligence Service [**CSIS** or **the Service**] to keep pace. However, it must do so within the bounds of the law.

[2] There are two principal issues in this proceeding. The first is whether CSIS may deploy a particular new technology [the **Technology**] within Canada in four specific ways without a warrant, in the course of investigations pursuant to section 12 of the *Canadian Security*

Intelligence Service Act, RSC 1985, c C-23 [the ***CSIS Act***]. Three of those proposed uses of the Technology would be solely within Canada, while the fourth would be both within and outside Canada.

[3] The Attorney General of Canada [**AGC**] concedes that the utilization of the Technology solely within Canada in each of those four proposed ways would constitute a "search," within the meaning of section 8 of the *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 [the ***Charter***]. However, the AGC maintains that those ways of deploying the Technology would not be "unreasonable," as contemplated by section 8. This is because (i) they would be "minimally intrusive", and therefore authorized by section 12 of the *CSIS Act*; (ii) section 12 is a reasonable law; and (iii) the "searches" would be carried out in a reasonable manner.

[4] For the reasons that follow, I agree. The Technology may be deployed within Canada in the four specific ways that CSIS has proposed, without a warrant, provided that such uses of the Technology are consistent with the reasons set forth below, particularly paragraphs 62, 88, 116–117, 126–127 and 141.

[5] The second principal issue in this proceeding is whether CSIS may utilize the Technology outside Canada against foreign nationals with no recognized nexus to Canada, without a warrant. This use of the Technology would be more than minimally intrusive. However, for the reasons provided below, I have concluded that CSIS would not require a warrant before deploying the Technology outside Canada in the ways that it has identified.

[6] In brief, foreign nationals with no recognized nexus to Canada do not benefit from the protections afforded by section 8. This includes the requirement for pre-authorization of a search by an entirely neutral and impartial arbiter who is capable of acting judicially in balancing the interests of the state against those of the individual, in certain circumstances: *Hunter et al v Southam Inc*, [1984] 2 SCR 145, at 160–162 and 168–9 [***Hunter***]. The Court's attention was not directed towards any principle of international law that would prevent CSIS from deploying the Technology outside Canada in the manner it has identified, without a warrant and against such individuals.

[7] Given the confidential nature of the Technology, my detailed description of it is provided in Appendix I to these reasons, which will remain classified. The more basic description of the Technology set forth in the main body below is provided in a manner that will permit the public to understand the issues raised in this proceeding, despite the fact that redactions will nonetheless be necessary in the public version of this decision, for national security reasons.

II. **Background**

A. *Principal Uses of the Technology and Procedural History*

[8] In December 2021, the Court received a supplemental warrant application in which CSIS sought warrant powers to deploy a new technological tool against existing targets of an investigation being conducted pursuant to section 12 of the *CSIS Act*. The new tool is a [...] technology [...] that has [...] capabilities. These include the ability to identify [...] [a

Device] [...]. They also include the ability [...] a Device. Such [...] information can be obtained by identifying [...] associated with a Device.[1]

[9] At the present time, [...] in respect of which such information [...] may be obtained ranges from [...] with the Technology.

[10] [...] Such information can assist CSIS to make inferences about the [...] of those individuals, so as to advance investigational goals. The amount of information that can be obtained about a subject of investigation will depend on [...].

[11] CSIS is also able to use the Technology to identify [...] and to learn about [...]. In addition, the Technology can assist CSIS to identify [...], as well as to [...]. Other potential uses of the technology are briefly described in Appendix I below.

[12] In written submissions, counsel for the AGC submits that the Technology can be deployed within Canada in four specific ways that are minimally intrusive, such that those uses would be authorized under section 12 of the *CSIS Act*, without the need for a warrant. The first three of those ways would be solely within Canada, whereas the fourth would involve collecting [...] information from a Device [both within and outside Canada]. An important aspect of the AGC's position in this regard is its assertion that the four methods of utilizing the Technology in Canada without a warrant would not involve the [...].

---

[1] [...]

[13] The AGC further submits that foreign nationals abroad who have no nexus to Canada do not benefit from the protections afforded by section 8 of the *Charter*. Therefore, the AGC asserts that CSIS may deploy the Technology against such persons in more intrusive ways, without a warrant. Such more intrusive ways include [...].

[14] Notwithstanding the foregoing, CSIS sought a Provisional [...] Warrant [**Provisional Warrant**] to enable it to obtain the [...] of several named subjects within Canada, *for the purposes of* [...] *to those persons*. In its initial correspondence to the Court in relation to that warrant, the AGC explained that the requested powers "could be justified as minimally intrusive under s. 12 of the CSIS Act, without the need for a warrant." However, the warrant was being sought out of an abundance of caution, to avoid inadvertently violating the *Charter* while (i) CSIS gained a better understanding of the data that would be returned through the [Technology], and (ii) the Court considered whether that particular use of [...] data could be authorized under s. 12 of the *Canadian Security Intelligence Service Act* alone. The AGC reserved the right to return to the Court at a later date to argue that the requested powers do not require a warrant, for the reason explained above.

[15] During the hearing of the Provisional Warrant Application on January 25, 2022, I raised initial concerns regarding the potential for [...] data of Devices of third parties to be incidentally obtained in the course of exercising the warranted powers. To substantially reduce the scope for this to occur, I insisted that the warrant be amended to provide the authority to obtain [...] identified in the warrant, for each of the named subjects of investigation. After

unsuccessfully endeavouring with counsel to identify a similar limiting mechanism for other provisions of the requested warrant, those other provisions were deleted.

[16] On the same date that the Provisional Warrant was issued, I issued a second warrant, described as [...] Warrant. That warrant authorized CSIS to deploy the Technology in a manner that CSIS acknowledged was more than minimally intrusive, including [...] of the Devices of the same named subjects of investigation who were identified in the Provisional Warrant.

[17] Each of the two above-mentioned warrants expired on February 26, 2022. However, new warrants with some amendments that are not relevant for the present purposes were issued by Justice Norris on February 24, 2022. Those warrants were issued on the understanding that CSIS would bring an application to cancel or amend the extended Provisional Warrant based on the present decision.

[18] To assist the Court in addressing the legal issues raised by this application, I appointed Mr. Gib van Ert as *amicus curiae* [the ***Amicus***].

B. *CSIS's Pilot Project and NSIRA's Review*

[19] CSIS first used the Technology on a pilot basis for several months in 2018. During that period, it was used without a warrant approximately [...] times against Canadian and non-Canadian subjects of investigation located in Canada and abroad. A total of [...] operational reports [...] resulted from those uses of the Technology. However, after privacy issues were

raised internally, the pilot project was terminated in July 2018. After that time, use of the Technology was confined to investigative activities in relation to (i) foreign nationals located outside Canada without a nexus to Canada, and (ii) [...]. In July 2020, CSIS suspended all use of the Technology until it obtained further clarity about the application of section 8 of the *Charter* to its collection activities against foreign nationals with no nexus to Canada.

[20] In mid-to-late 2018, the Security Intelligence Review Committee [**SIRC**] initiated a review of CSIS's use of the Technology earlier that year, during the above-mentioned pilot period. That review was ultimately completed by SIRC's successor, the National Security and Intelligence Review Committee [**NSIRA**], which issued a report entitled *Review of CSIS's Use of* [...] *– a Geolocation Data Collection Tool* (NSIRA Study 2018-05) [**NSIRA Report**]. That report was "communicated" to the Minister of Public Safety and Emergency Preparedness in August 2019.

[21] Among other things, NSIRA found that the use of the Technology [...] constituted a "search" for the purposes of section 8 of the *Charter*. NSIRA added that "there was a risk that CSIS breached section 8 of the Charter during the trial period in which it used [the Technology] without a warrant": NSIRA Report, at 11. NSIRA proceeded to recommend as follows:

> " … that CSIS review its use of [the Technology] to date and make a determination as to which of the operational reports generated through the use of [the Technology] were in breach of section 8 of the Charter. These operational reports and/or any documents related to those results should be purged from its systems."

NSIRA Report, at 12.

[22] According to CSIS's technical affiant [**Affiant 1**], CSIS ultimately determined that the [...] above-mentioned operational reports needed to be retained in order to meet CSIS's legal obligations. Those reports and their attachments have been sequestered so as to ensure that the information contained therein does not inform or contribute to other CSIS investigations.

C. *CSIS's Delay in Informing the Court of its Use of the Technology Against Subjects of the Court's Warrants*

[23] I pause to observe that CSIS or the AGC ought to have informed the Court about the forthcoming NSIRA Report well before that report was released in August 2019. Their failure to do so before the present Application was filed more than two years later, in December 2021, was inconsistent with (i) a commitment made to the Court in 2016 by CSIS's Director, and (ii) the elevated duty of utmost good faith that applies in *ex parte* proceedings, particularly pursuant to the *CSIS Act*: *Canadian Security Intelligence Services Act (CA) (Re)*, 2021 FCA 92, at para 126 [***CSIS Act (Re) 2021 FCA***].

[24] Specifically, CSIS's Director of the day Mr. Michel Coulombe committed to advise the Court "as soon as an issue comes up" in a review by the Security Intelligence Review Committee relating to matters involving this Court's warrants, "even if the report is not finalized": *En Banc* Hearing, June 10, 2016, Transcript at 18 and 55. This was on the understanding that the final report and recommendations might be different from the initial information that had been communicated to the Court. In 2018, CSIS's current Director reiterated a commitment to abide by the spirit of this undertaking.

[25] The AGC's explanations for the failure to inform the Court about the NSIRA Report prior to the present proceeding do not withstand scrutiny. To begin, the AGC maintained that (i) the warrants involved individuals who were, or later became, either warranted subjects of investigation or the subject of a warranted collection, and (ii) that the warrants were obtained and expired prior to the release of the NSIRA Report. However, this does not provide a basis for relieving CSIS from its commitment, or its elevated duty of candour.

[26] Of the warranted individuals discussed in the NSIRA report, [...]. [...] warrants issued against [...] were [...] during the period covered by NSIRA's review and [...] issued for a one-year period in July 2018. Another was renewed in June 2018 and expired in June 2019. Given that the NSIRA Report was released in August 2019, it is reasonable to infer that the issues it addressed had sufficiently ripened to have fallen within the scope of both the Director's above-discussed commitment to the Court and the elevated duty of good faith disclosure well before that date.

[27] As for the [...], the Technology was deployed against them outside Canada. Warrants against [...] of those individuals were sought in mid-2019, [...]. The warrant against the [...] individual was sought [...] the application in the present proceeding was filed. Yet, the use of the Technology against these [...] individuals and the [...] described above was not disclosed prior to May 18, 2022. Indeed, the Court may never have been made aware of the uses of the Technology against these individuals had I not issued a Direction requiring the AGC and the Service to advise as to whether the Technology had ever been used or directed against any target who either was, or is, the subject of warrants issued by this Court.

[28] The AGC further explained that the Court was not informed about the use of the Technology against the above-mentioned individuals because none of the information collected was ever relied upon in an application for warrants. However, as the AGC and CSIS have been repeatedly advised in the past, information concerning the techniques that have been used against subjects of investigation in respect of whom a warrant application has been made, or is being made, is relevant to both the exercise of the Court's discretion and its oversight of its outstanding warrants.

[29] As long as the information may be considered to be relevant to the Court's exercise of discretion to issue or revisit an outstanding warrant, it must be disclosed: *CSIS Act (Re) 2021 FCA*, at para 127. The duty of utmost good faith and transparency requires no less.

[30] This is so even if the information is or was not relied upon in the warrant application.

[31] For greater certainty, this remains true even if CSIS's affiant has determined that the information does not fall within the scope of the matters to be specified in an application for a warrant, as set forth in paragraphs 21(2)(a) and (b) of the *CSIS Act*: *CSIS Act (Re) 2021 FCA*, at para 133. This is so for two reasons. First, the information might well be relevant to the exercise of the Court's discretion. Second, the Court may well disagree with the determination of CSIS's affiant regarding the scope and applicability of paragraphs 21(2)(a) and (b).

[32] As a result of this Court's decision in *X (Re)*, 2020 FC 616, and general principles subsequently articulated in *CSIS Act (Re) 2021 FCA*, at paras 120–133, the AGC and CSIS now

recognize that the elevated duty of candour requires the disclosure of all information that may be relevant to the determinations this Court must make in deciding whether to issue a warrant, and if so, on what terms. This includes information that may not have been relied on in support of a warrant application. The AGC and CSIS also accept that NSIRA's finding that there was a risk of a breach of section 8 of the *Charter* in relation to CSIS's use of the Technology within Canada fell within the scope of the elevated duty of full and frank disclosure. They further acknowledge that the Court retains discretion, when informed of matters that fall within the scope of that duty, to rescind the ongoing validity of active warrants, to refuse to issue new warrants, or to order other relief.

III. **Issues**

[33] There are two principal issues in this proceeding. They are as follows:

1. Does section 12 of the *CSIS Act* authorize CSIS to utilize the Technology within Canada in the four ways CSIS has identified, without a warrant?

2. Does section 12 of the *CSIS Act* authorize CSIS to utilize the Technology outside Canada against foreign nationals with no nexus to Canada, and in the more intrusive ways it has identified, without a warrant?

IV. **Assessment of the proposed uses within Canada (Issue #1)**

A. *Summary of the Four Proposed Uses and Introduction*

[34] As previously noted, three of the proposed methods of deploying the Technology would be solely within Canada. They are as follows:

i) Against known targets of CSIS investigations, [...] within Canada [...].

ii) Against known targets of CSIS investigations, [...] within Canada, [...].

iii) [...] within Canada [...].

[35] The fourth proposed use of the Technology [...] would involve collecting [...] data from Devices [both within and outside Canada][2].

[36] The general legal principles applicable to CSIS's use of new technology to obtain information about the mobile communications devices of subjects of investigation were extensively reviewed in *X (Re)*, 2017 FC 1047 [***IMSI***]. There, the Court applied the jurisprudence pertaining to what constitutes a "search" and what constitutes an "unreasonable" search, within the meaning of section 8 of the *Charter*. Like the present proceeding, *IMSI* involved an application pursuant to sections 12 and 21 of the *CSIS Act.*

[2] [...]

[37] There, the Court determined that CSIS's use of a cellular-site simulator [**CSS**] to capture the identifying characteristics of a subject of investigation's mobile communications devices in Canada without a warrant constituted a "search," but not an "unreasonable" one. Those identifying characteristics consisted of the International Mobile Subscriber Identity and International Mobile Equipment Identity numbers that were emitted by the subject's devices at certain times.

[38] In *Canadian Security Intelligence Services Act (CA) (Re)*, 2020 FC 697 [CSIS_2020], the Court made similar findings regarding the use of (i) CSS technology to capture the same information that was at issue in *IMSI* [_..._]. However, it proceeded to find that CSIS requires a warrant to [_..._] obtain information about individuals [_..._], which reveals much more personal information about the user of a communications device: [CSIS_2020], at paras 118–125, 166–169 and 176–181. Those findings were made in the context of an application under sections 16 and 21 of the *CSIS Act*.

[39] In *IMSI*, the Court's conclusion that the capture of the identifying characteristics of the target's mobile device did not constitute an "unreasonable" search was based on three principal findings: (i) the "search" was authorized by law, namely, section 12 of the *CSIS Act*, (ii) that law is reasonable, and (iii) the searches would be carried out in a reasonable manner: *IMSI*, at paras 198–201, 236 and 238–243.

[40] Section 12 states as follows:

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 Government of Canada.	**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 Canada et le conseille à cet égard.
No territorial limit	**Aucune limite territoriale**
(2) For greater certainty, the Service may perform its duties and functions under subsection (1) within or outside Canada.	(2) Il est entendu que le Service peut exercer les fonctions que le paragraphe (1) lui confère même à l'extérieur du Canada.

[41] In the course of assessing the authority provided by section 12, the Court in *IMSI* noted the following:

> [196] The plain language of section 12 requires CSIS to collect, by investigation or otherwise, to the extent that it is strictly necessary, and to analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada. This provides CSIS with the explicit authority to investigate such threats in those circumstances.

[42] The Court proceeded to observe that section 12 authorizes CSIS to collect, analyse and retain information that ranges from non-intrusive to highly intrusive. However, once CSIS "moves beyond minimally invasive collection activities, it will require a warrant": *IMSI*, above, at para 219. It is important to keep in mind that this statement was made in the context of the Court's assessment of the application of section 8 of the *Charter* to intrusive activity in which CSIS had engaged *within* Canada. In that context, and given the provisions of section 21 pertaining to warrants, it could be inferred that Parliament implicitly contemplated that CSIS would require judicial preauthorization before engaging in collection activities that were more than minimally intrusive: *IMSI*, above, at para 219.

[43] It is common ground between the AGC and the *Amicus* that the Court's decision in *IMSI* provides an appropriate point of departure for the analysis of some of the important issues in the present proceeding.

[44] In conducting the assessment below, I will remain mindful of the need to adopt "a purposive approach to section 8 that emphasizes the protection of privacy as a prerequisite to individual security, self-fulfilment and autonomy as well as to the maintenance of a thriving democratic society": *R v Spencer*, 2014 SCC 43, at para 15.

B. *Would the proposed uses of the Technology within Canada constitute a "search"?*

[45] In *IMSI*, the Court found that the target had a reasonable expectation of privacy [**REP**] in respect of the identifying characteristics of his mobile devices: *IMSI*, above, at paras 140, 177 and 189. This REP existed because of the nature of the information that CSIS was able to begin

learning about his private activities, upon obtaining those numeric identifiers from his devices. CSIS's intrusion on this REP constituted a "search" within the meaning of section 8 and therefore "engaged" the privacy interests protected therein: *IMSI*, above, at paras 111, 149 and 247.

[46] In the present proceeding, it is common ground between the AGC and the *Amicus* that each of the four ways in which CSIS proposes to utilize the Technology within Canada would constitute a "search" within the meaning of section 8. This is because individuals in Canada have an REP in the [...] data [...] that are accessible through the Technology. However, the AGC and the *Amicus* disagree about whether the use of the Technology outside Canada in relation to foreigners who have no nexus to Canada, would constitute such a "search". This will be discussed in part IV.C. (3)(d) below.

C. *Would the Proposed Uses of the Technology Within Canada Constitute an "Unreasonable" Search?*

[47] Warrantless searches such as those proposed in the present proceeding are presumptively unreasonable. However, that presumption may be rebutted by demonstrating that: (i) the searches are authorized by law, (ii) the law is reasonable, and (iii) the searches will be carried out in a reasonable manner: *Spencer*, at para 68.

(1) Are the proposed searches authorized by law?

[48] It is common ground between the AGC and the *Amicus* that the four proposed uses of the Technology within Canada would be authorised by section 12 of the *CSIS Act*, so long as they are only minimally intrusive in nature. The *Amicus* maintains that this would be the case only if

CSIS abides by certain conditions that are discussed in section IV.C. (3) below, which addresses the reasonableness of the proposed searches.

(2) Is the authorizing law reasonable?

[49] The AGC and the *Amicus* agree that section 12 is a reasonable law. However, the *Amicus* maintains that the analysis of this second prong of the tripartite test for assessing the reasonableness of the proposed searches should not end there. Instead, the *Amicus* submits that the Court's assessment should include a review of the [...] as well as the [...].

[50] With respect to the [...], the *Amicus* submits that they do not reasonably contemplate the use of [...] data for national security purposes.

[51] In support of this position, the *Amicus* notes that the NSIRA Report made the following observation at page 6:

[...].

[52] The *Amicus* further notes that similar observations were made in several of the [...] that were attached to one of the affidavits sworn by Affiant 1. In this regard, the *Amicus* quoted the following statement regarding the data available through the Technology: [...][3]

[53] [This paragraph describes a legal argument put forward by the *Amicus* as to whether an instrument, other than an act or regulation, must be considered in addition to s.12 of the *CSIS Act*

[3] [...]

in assessing whether the deployment of the tool is authorized by law. *Amicus* submits that consideration of the instrument supports a conclusion of unreasonableness for the purposes of the Court's inquiry under section 8 of the *Charter*.]

[54] In reply, the AGC submits that, for the purposes of section 8, [...] are only potentially relevant to the assessment of whether intrusive investigative activity constitutes a "search." They are not relevant to the assessment of whether a "search" is unreasonable, unless there is evidence of unlawful activity. The AGC observes that, in the case at hand, there is no such evidence — either in respect of the acquisition of [...] data [...]. Indeed, to the extent that there is any relevant evidence in this regard, it points in the opposite direction. In particular, a document [...] entitled [...] states: "all data collection is done legally [...][4].

[55] The AGC maintains that the *Amicus*' position on this issue confuses lack of waiver of a REP with reasonable lawful authority to intrude upon a REP. The latter does not depend on a user consenting to or reasonably expecting such an intrusion. The AGC contends that if there was no REP, there would be no "search" and therefore no need to assess the reasonableness of the authorizing law.

[56] In support of this position, the AGC notes that in *IMSI* this Court found that the interception of mobile device identifiers without a warrant was lawful, even though [...]. In other words, [...] were not relevant to the assessment of [...].

---

[4] [...]

[57] The AGC further observes that, in the criminal law context, the Supreme Court of Canada [**SCC**] has acknowledged that police "may employ creativity and subterfuge" and "resort to tricks or other forms of deceit" in conducting their investigations: *R v Mills*, 2019 SCC 22, at para 43; *Rothman v The Queen*, [1981] 1 SCR 640, at 697.

[58] [This paragraph describes the Court's finding that the instrument was relevant to the assessment of whether a device user has an REP in their data but was not relevant to the assessment of whether CSIS proposed intrusions on any REP are authorized by a reasonable law.]

[59] Given the foregoing, and given the *Amicus*' acknowledgment that section 12 of the *CSIS Act* is a reasonable law, it follows that the law authorizing the proposed "searches" is reasonable.

(3) Would the searches be carried out in a reasonable manner?

(a) *The First Proposed Use of the Technology Within Canada*

(i) Subjects of Investigation

[60] In this scenario, the Technology would be used against known targets of CSIS investigations, by [...].

[61] This proposed warrantless use of the Technology is the same as that which was before me in respect of the Provisional Warrant, discussed at paragraphs 14-15 above. As discussed, CSIS sought that warrant out of an abundance of caution, to ensure that it did not inadvertently violate the *Charter* while (i) it gained a better understanding of the data that would be returned through

the [Technology], and (ii) the Court considered whether that particular use of [...] data could be authorized under s. 12 of the *Canadian Security Intelligence Service Act* alone. At that time, CSIS also explicitly reserved its right to return to the Court to argue that this use of the Technology was minimally intrusive and therefore did not require a warrant.

[62] For many of the same reasons discussed in *IMSI* and [CSIS 2020] this proposed manner of utilizing the Technology (i) is minimally intrusive of the informational and territorial privacy interests of CSIS's subjects of investigation, and (ii) would not give rise to an "unreasonable" search within the meaning of section 8 of the *Charter*: *IMSI*, above, at paras 161–163 and 187–189; [CSIS 2020], above, at 124–125 and 166–168. Consequently, this use would be authorized under section 12 of the *CSIS Act*, without the need for a warrant. This is subject to the requirement to destroy information that is incidentally collected from non-threat-related third parties quickly, and before assessing that information in any manner whatsoever. I will return to this point in the next section below.

[63] When utilizing the Technology in the manner contemplated by this first proposed use within Canada, CSIS would be seeking information about known subjects of investigation [...] CSIS could then seek a warrant [...].

[64] In the absence of such a warrant, the [...] data obtained by CSIS through the Technology would be very limited. At most, it could consist of [...]. While CSIS's access to this [...] data would intrude upon the target's reasonable expectation of privacy in data [...] from [...] such intrusion would be minimal in nature [...].

[65] As in *IMSI*, CSIS would not be able to access any communications made with the Devices, or any information stored on or accessible through the Devices. Moreover, this proposed use of the Technology would not reveal anything about the activities of CSIS's subjects of investigation. [...] there would be no impact on the target's experience when using the Devices in question.

[66] It bears underscoring that the AGC acknowledges that CSIS would not be able to use the Technology to [...] without a warrant. [...]. Consequently, use of the Technology for such purposes would require a warrant.

[67] I recognize that CSIS's linking of [...] a target's [...] Device may well assist CSIS to begin putting together a personal "profile" of the target, or to add to any profile that it may have already begun to build. However, it is difficult to see how the inferences it may be able to draw regarding the target's personal activities would be particularly strong or invasive: *IMSI*, above, at paras 163 and 189; [CSIS 2020], above, at paras 123–125 and 166–168. I am satisfied that any such inferences would not extend to "core" biographical information about the target. [...].

[68] As in *IMSI* and [CSIS 2020], the fact that this proposed use of the Technology is minimally intrusive, highly accurate and narrowly focused, significantly assists to support a finding that the "search" is not unreasonable: *IMSI*, above, at paras 7, 207, 209 and 236(i); [CSIS 2020], above, at paras 123–125, 161 and 166–168. This high accuracy and narrow focus includes the information obtained by CSIS [...] which is further circumscribed by the [...] criteria that would be specified in utilizing the Technology to obtain the desired results.

[69] I will pause to add that I do not place great significance on the fact that the [...] data accessible through the Technology is [...]. This is so for two reasons. First, that information [...]. Second, the nature of the information obtained is such that its (minimal) degree of its intrusiveness does not materially change by virtue of the fact that it is [...]. In other words, there is nothing about the nature of a Device [...]. In both cases, the capture is equally intrusive, albeit minimally so.

(ii) Non-threat-related Third Parties

[70] One of the unfortunate costs of certain legitimate investigative techniques is that private information of "innocent" third parties may be unavoidably captured: *R v Thompson*, [1990] 2 SCR 1111, at 1143–44 [***Thompson***]. Consequently, in warrant applications under the *CSIS Act*, this Court has steadfastly endeavoured to minimize such incidental intrusions on the privacy interests of third parties. Stated differently, the Court has sought to ensure that the incidental collection of third party information is not more intrusive or more broad than what is reasonably required to achieve CSIS's legitimate investigative objectives: *IMSI*, above, at para 253.

[71] In some cases involving the investigation of data pertaining to mobile communications devices, courts have recognized that it may be reasonably necessary to authorize the capture of a small amount of minimally intrusive data pertaining to a very large number of third parties: *IMSI*, above, at paras 66–67; *R v Baskaran*, 2020 ONCA 25, at paras 18 and 21–23 [***Baskaran***]; *R v Brewster*, 2016 ONSC 4133, at paras 60–62 [***Brewster***].

[72] This acceptance of the practical necessity of broad capture of minimally intrusive information at the authorization stage has been counterbalanced by ensuring that information pertaining to non-threat-related third parties is quickly destroyed and, where reasonably possible, not subjected to any analysis whatsoever: *IMSI*, above, at paras 5, 156 and 252–254; [...] [CSIS 2020] above, at paras 17 and 168; *X (Re)*, 2016 FC 1105 at paras 186–188; Sections 12 and 21 of the *Canadian Security Intelligence Service Act, RSC 1985, c C-23 (Re)*, 2019 FC 141, at paras 32 and 37–39 [***CSIS Act (Re) 2019***].

[73] In this context, "non-threat-related third parties" means individuals who are not involved in threats to the security of Canada, as defined in section 2 of the *CSIS Act*.

[74] In the case at hand, each of the four proposed uses of the Technology within Canada is likely to result in the incidental collection of [...] data pertaining to Devices of non-threat-related third parties. An exception would be where the Technology is deployed in relation to [...].

[75] Fortunately, CSIS has a strong incentive to deploy the Technology in a manner that minimizes the [...] data is collected. [...].

[76] Moreover, in certain situations, third party [...] data can be readily identified and quickly destroyed without any adverse impact on CSIS's investigation. [...]. As in *IMSI* [...] *IMSI*, above [...].

[77] For this reason, in considering the Provisional Warrant that I granted on January 25, 2022 (see paras 14-15 above), I insisted on the insertion of [...] requirement. In brief, the authorization to utilize the Technology was limited to situations in which [...] data could be obtained in relation to [...] identified in the warrant, for each named subject of investigation. As in *IMSI*, the data obtained [...] would then be quickly destroyed pursuant to one of the conditions in the warrant, without being subjected to any analysis whatsoever: *IMSI*, above, at paras 5, 7, 156, 236(i), 242 and 253.

[78] Subsequent to the issuance of the Provisional Warrant, the AGC filed additional submissions. Among other things, those submissions maintained that restricting the use of the Technology to [...] would create unacceptable investigative blind spots and would stymie CSIS's investigation. In this regard, the AGC cited the following passage from *R v Vu*, 2013 SCC 60, at para 57:

> In short, attempts to impose search protocols during the authorization process risk creating blind spots in an investigation, undermining the legitimate goals of law enforcement that are recognized in the pre-authorization process. These problems are magnified by rapid and constant technological change.

[79] The AGC noted that similar observations were made in *R v Latimer*, 2020 BCSC 2173, at para 101.

[80] In further support of its position, the AGC gave two examples. The first concerned an investigation of [...]. In this situation, the AGC asserted that it would be entirely possible that

CSIS would [...]. In the second example, the AGC posited [...]. The clear implication was that innocent lives could be at stake in the meantime.

[81] Based on the foregoing, and upon further consideration, I agree that it would not be appropriate to impose a [...] requirement in connection with the first of the proposed uses of the Technology, or indeed with respect to any of the three other proposed uses, within Canada. I will note for the record that the *Amicus* expressed the same view.

[82] I am satisfied that the nature of the Technology is such that CSIS will be highly incentivized to use [...] whenever reasonably possible. This is because that manner of proceeding would enable CSIS to rapidly identify the [...] data of its subjects of investigation [...]. When [...] data pertaining to Devices of third parties can be readily identified and quickly destroyed, without the need for any analysis whatsoever. In these circumstances, any intrusions upon the privacy rights of third parties would be temporary and limited [...].

[83] This very small intrusion into the privacy rights of third parties would not be unreasonable. This is because it would be outweighed by the value of the intelligence that the Technology would enable CSIS to obtain: *IMSI*, above, at para 211. Moreover, the [...] parameters that would be used when deploying the Technology would collectively serve to minimize the extent to which [...] data is even temporarily collected. As in *IMSI*, such narrow targeting, combined with the highly accurate and minimally intrusive nature of the proposed uses of the Technology, weigh in favour of concluding that they would not unreasonably intrude upon the privacy rights of third parties.

[84] A further factor that will assist to ensure that such intrusions are not unreasonable is that the Technology can only be deployed when the requirements of section 12 of the *CSIS Act* are satisfied. These include the necessity for CSIS to have "reasonable grounds to suspect" and the requirement that the use of the Technology be "strictly necessary." In addition, [...] would have direct access to the [...] results obtained through the Technology. In this regard, Affiant 1 testified that [...] individuals within CSIS currently have the [...] necessary to use the Technology: February 9, 2021 Hearing Transcript at 95; see also *Brewster*, above, at paras 60–62. He added that only those individuals would [...] collected [...] in deploying the Technology for the first of the uses that CSIS has proposed in this proceeding. Likewise, they are the only persons who would assess whether [...] collected in the second and third scenarios discussed below were threat-related [...] for retention purposes, although I note that they may consult the operational desk in conducting that assessment.

[85] I will now turn to situations in which the Technology cannot reasonably be deployed in relation to [...]. During the hearing on the Provisional Warrant, I raised the possibility of imposing a cap on the total number of third parties whose [...] data could be obtained through the use of the Technology in relation to [...]. Once again, the AGC took the position that this could significantly reduce the potential utility of the Technology. Using the second of the two examples discussed above, concerning [...] the AGC maintained that the imposition of such a cap would [...].

[86] More generally, the AGC insisted that using the Technology in respect of [...] does not, in and of itself, result in impermissible bulk collection or render the search unreasonable on the

basis of overbreadth. This would be so even if use of the Technology in relation to [...] yielded [...] data relating to a large number of innocent third parties. The *Amicus* agreed.

[87] The AGC added that, as a practical matter, for the first of the three uses of the Technology solely within Canada, the volume of third party data collected [...] "would likely be minimal if any." This is because the Technology would [...] to a subject of investigation, if it were used in respect of [...] third parties were likely to be present. In such situations, [...] would be returned by the [Technology].

[88] Having regard to the foregoing, I am satisfied that it would not be appropriate to impose an arbitrary upper limit on the number [...] when deploying the Technology. This is so even when the Technology is deployed in relation to [...]. However, in all circumstances, any [...] data that is obtained in relation to the Devices of non-threat-related third parties must be quickly destroyed before being subjected to any analysis whatsoever: see paragraph 62 above and paragraphs 116–117 and 126–127 below. For greater certainty, and as discussed in the next section below, this means that CSIS cannot run incidentally collected third party information through its section 12 databases.

[89] In making this determination, I have been given greater comfort by the fact that CSIS will have a strong "built-in" incentive to deploy the Technology in a manner that minimizes the number of Devices of non-threat-related persons in respect of whom [...] data is collected. As discussed, this is because [...]. In the latter case, the use of the Technology would effectively achieve the objective of the second proposed use, discussed in the next section below.

[90] In summary, for the reasons set forth above, the first proposed use of the Technology within Canada would not constitute an "unreasonable" intrusion on the privacy rights of non-threat-related parties. This is so even in situations in which [...] data may be obtained in relation to a large number of non-threat-related third parties.

(iii) Cross-checking Incidentally Collected Data Against Previously Collected Information

[91] In the AGC's supplemental written submissions, the AGC noted that CSIS might run incidentally collected [...] through its section 12 databases to determine if any were threat-related. If so, such threat-related [...] would be ingested into CSIS's holdings and subject to future querying.

[92] In my view, such cross-checking against previously collected information would be inconsistent with the stated purpose of the first proposed use of the Technology. That purpose was represented to be confined to [...] a known subject of investigation. This cross-checking would also be inconsistent with the AGC's representation that CSIS [...]. The AGC added:

[...].

[93] Where CSIS is able to conduct a [...]. All [...] data obtained in respect of other Devices [...] can and should be quickly destroyed without further analysis. The same is true with respect to the "[...] circumstances" where CSIS would use the Technology to [...]. This is because the AGC represented that such circumstances would be limited to where CSIS reasonably suspects that either the subject of investigation [...] run incidentally collected [...] through its section 12 database would be akin to authorizing a fishing expedition. That would not

be reasonable: *Hunter*, above, at 167; *Thompson*, above, at 1145. For greater certainty, this observation is confined to the first of the three uses of the Technology within Canada that have been proposed.

(iv) The *Amicus*' Proposed Conditions

[94] The *Amicus* submits that none of the proposed uses of the Technology would be carried out in a reasonable manner without the imposition of specific limitations on CSIS's ability to (i) share [...] data, and (ii) retain incidentally collected [...] data pertaining to innocent third parties. More specifically, for each of the proposed uses of the Technology within Canada, the *Amicus* maintains that they can only be conducted in a way that is minimally intrusive of section 8 rights on the following conditions:

(a) Collected [...] data [...] is not shared with domestic or foreign agencies; and

(b) Incidentally collected data (i.e., data relating to persons who are not reasonably suspected to be threats to the security of Canada) is deleted as soon as possible without being uploaded into Service holdings.

[95] Regarding the sharing of [...] data, the *Amicus* maintains that CSIS has no power to control the manner in which its security partners may use shared data, particularly with respect to foreign partners. This was acknowledged by the principal affiant [**Affiant 2**], who also conceded that he did not know whether CSIS has a policy pursuant to which foreign partners are advised when CSIS concludes that [...] that has been shared is not threat-related.

[96] Consequently, the *Amicus* states that sharing opens the way to uses of [...] data that the Court can neither anticipate nor control. This includes uses that might be very harmful to the individuals concerned. Without any limitation on such sharing, the Court cannot conclude that

the proposed uses of the Technology would be "minimally intrusive." Therefore, the *Amicus* maintains that in the absence of any need to share [...] for the purpose of [...] CSIS should be prevented from engaging in such sharing.

[97] In reply, the AGC submits that a prohibition on sharing [...] data with domestic and foreign partners would be contrary to the *CSIS Act* and the governing jurisprudence. I agree.

[98] Section 19 of the *CSIS Act* states as follows:

Authorized disclosure of information	**Autorisation de communication**
19(1) Information obtained in the performance of the duties and functions of the Service under this Act shall not be disclosed by the Service except in accordance with this section.	**19(1)** Les informations qu'acquiert le Service dans l'exercice de ses fonctions qui lui sont conférées en vertu de la présente loi ne peuvent être communiquées qu'en conformité avec le présent article.
Idem	**Idem**
(2) The Service may disclose information referred to in subsection (1) for the purposes of the performance of its duties and functions under this Act or the administration or enforcement of this Act or as required by any other law and may also disclose such information,	**(2)** Le Service peut, en vue de l'exercice des fonctions qui lui sont conférées en vertu de la présente loi ou pour l'exécution ou le contrôle d'application de celle-ci, ou en conformité avec les exigences d'une autre règle de droit, communiquer les informations visées au paragraphe (1). Il peut aussi les communiquer aux autorités ou personnes suivantes :
(a) where the information may be used in the investigation or prosecution of an alleged contravention of any law of Canada or a province, to a peace officer having jurisdiction to investigate the alleged contravention and to the Attorney General of Canada and the Attorney General of the province in	**(a)** lorsqu'elles peuvent servir dans le cadre d'une enquête ou de poursuites relatives à une infraction présumée à une loi fédérale ou provinciale, aux agents de la paix compétents pour mener l'enquête, au procureur général du Canada et au procureur général de la

which proceedings in respect of the alleged contravention may be taken;	province où des poursuites peuvent être intentées à l'égard de cette infraction ;
(b) where the information relates to the conduct of the international affairs of Canada, to the Minister of Foreign Affairs or a person designated by the Minister of Foreign Affairs for the purpose;	**(b)** lorsqu'elles concernent la conduite des affaires internationales du Canada, au ministre des Affaires étrangères ou à la personne qu'il désigne à cette fin ;
(c) where the information is relevant to the defence of Canada, to the Minister of National Defence or a person designated by the Minister of National Defence for the purpose; or,	**(c)** lorsqu'elles concernent la défense du Canada, au ministre de la Défense nationale ou à la personne qu'il désigne à cette fin ;
(d) where, in the opinion of the Minister, disclosure of the information to any minister of the Crown or person in the federal public administration is essential in the public interest and that interest clearly outweighs any invasion of privacy that could result from disclosure, to that minister or person.	**(d)** lorsque, selon le ministre, leur communication à un ministre ou à une personne appartenant à l'administration publique fédérale est essentielle pour des raisons d'intérêt public et que celles-ci justifient nettement une éventuelle violation de la vie privée, à ce ministre ou à cette personne.
Report to the Review Agency	Rapport à l'Office de surveillance
(3) The Director shall, as soon as is practicable after a disclosure referred to in paragraph 2(d) is made, submit a report to the Review Agency with respect to the disclosure.	**(3)** Dans les plus brefs délais possible après la communication visée à l'alinéa (2)d), le directeur en fait rapport à l'Office de surveillance.

[99] As is apparent from the foregoing, subsection 19(2) authorizes CSIS to disclose information obtained in the performance of its duties and functions under that legislation, for several specific purposes. These include (i) the performance of its duties and functions under the *CSIS Act*; (ii) the administration or enforcement of that legislation; (iii) as required by any other law; and (iv) in the specific circumstances described in paragraphs 19(2)(a) – (d).

[100] The AGC recognizes that these provisions constrain CSIS's ability to share [...] data collected without a warrant under section 12. In particular, the AGC acknowledges that CSIS would not be able to share such information, domestically or with foreign partners, unless: (i) it was assessed as threat-related, or (ii) it otherwise met the narrow requirements specified in subsection 19(2).

[101] Having regard to the AGC's representations, it would appear that the risk of non-threat-related [...] data being disclosed to a foreign partner, or to a domestic partner outside the restricted circumstances described in that provision, would be very low. This is because such disclosure would presumably be confined to situations where the information was mistakenly assessed as threat-related.

[102] More generally, section 17 of the *CSIS Act* permits CSIS to cooperate with domestic and foreign state actors, subject to ministerial approval. That provision states:

Cooperation	**Coopération**
17(1) For the purpose of performing its duties and functions under this Act, the Service may,	**17(1)** Dans l'exercice des fonctions qui lui sont conférées en vertu de la présente loi, le Service peut :
(a) with the approval of the Minister, enter into an arrangement or otherwise cooperate with	**a)** avec l'approbation du ministre, conclure des ententes ou, d'une façon générale, coopérer avec :
(i) any department of the Government of Canada or the government of a province or any department thereof, or	**(i)** les ministères du gouvernement du Canada, le gouvernement d'une province ou l'un de ses ministères,
(ii) any police force in a province, with the approval of	**(ii)** un service de police en place dans une province avec l'approbation du ministre

the Minister responsible for policing in the province; or	provincial chargé des questions de police ;
(b) with the approval of the Minister after consultation by the Minister with the Minister of Foreign affairs, enter into an agreement or otherwise cooperate with the government of a foreign state or an institution thereof or an international organization of states or an institution thereof.	**(b)** avec l'approbation du ministre, après consultation entre celui-ci et le ministre des Affaires étrangères, conclure des ententes ou, d'une façon générale, coopérer avec le gouvernement d'un État étranger ou l'une de ses institutions, ou une organisation internationale d'États ou l'une de ses institutions.
Copies of arrangements to Review Agency	Transmission des ententes à l'Office de surveillance
(2) Where a written arrangement is entered into pursuant to subsection (1) or subsection 13(2) or (3), a copy thereof shall be given forthwith to the Review Agency.	**(2)** Un exemplaire du texte des ententes écrites conclues en vertu du paragraphe (1) ou des paragraphes 13(2) ou (3) est transmis à l'Office de surveillance immédiatement après leur conclusion.

[103] The public interest in CSIS being able to share information with foreign partners has been repeatedly recognized by this Court and by the Federal Court of Appeal [**FCA**]: see for example, *Mahjoub (Re)*, 2013 FC 1096 [***Mahjoub***], at paras 57–58 and 63; *Canada (Attorney General) v Almalki*, 2010 FC 1106, at para 131; and *Canada (AG) v Charkaoui*, 2018 FC 849, at paras 151 and 155. The FCA has also noted the importance of the "give to get" principle: *Mahjoub v Canada (Citizenship and Immigration)*, 2017 FCA 157 at para 287 [***Mahjoub FCA***]. This principle was also implicitly recognized by the SCC in the context of Canada being a "net importer" of national security information, where the Court noted the state's interest in preserving Canada's present supply of intelligence received from foreign sources: *Ruby v Canada (Solicitor General)*, 2002 SCC 75, at paras 43–44.

[104] In *Mahjoub FCA*, at paragraph 179, the FCA added that "[t]he intelligence sharing scheme under the [CSIS Act] is subject to various safeguards and oversight and does not in principle […] result in unreasonable searches in violation of the Charter …"

[105] I will add in passing that, in *IMSI*, this Court concluded that CSIS could intercept identifiers from mobile communications devices without a warrant, despite the possibility that such information could be shared with foreign agencies and despite the potential consequences for the individuals in question: *IMSI*, above, at paras 146 and 168.

[106] Given the foregoing, I consider that it would not be appropriate to limit CSIS's ability to share [...] data with foreign or domestic partners. In reaching this conclusion, I consider it to be appropriate to underscore the AGC's acknowledgement that CSIS would not be able to share such information unless: (i) it was assessed as threat-related, or (ii) it otherwise met the narrow requirements specified in subsection 19(2). During oral submissions, the AGC's representative emphasized that "non-threat-related information can never be shared with foreign agencies and, by and large, it can't be shared with other Canadian agencies, except in those four very narrowly circumscribed scenarios under section 19(2)(a) to (d)": see March 23, 2021 Hearing Transcript, at 168.

[107] I will now turn to the *Amicus* proposed condition regarding the retention of incidentally collected data (i.e., non-threat-related data). That condition would require CSIS to delete incidentally collected [...] data "as soon as possible without being uploaded into [CSIS's] holdings."

[108] In support of this proposal, the *Amicus* notes that Affiant 1 testified that the duration of the retention period for [...] data obtained through the Technology would depend on the amount of time that it would take for CSIS to conduct its analysis. Typically, that would be "within days to weeks." However, Affiant 1 noted that it sometimes takes longer. When pressed on this, he stated: "There could be certain circumstances where it might be necessary to retain it for a longer length of time, into the [...]": March 23, 2021 Hearing Transcript, at 248. When further pressed as to whether he could foresee the retention period [...], he responded in the affirmative but acknowledged that this would be exceptional.

[109] Notwithstanding the foregoing, the AGC maintains that the proposed condition is not necessary for two reasons.

[110] First, the AGC states that the "strictly necessary" language in section 12 of the *CSIS Act* effectively prevents CSIS from retaining information that is non-threat-related, except in accordance with the dataset regime in sections 11.01 to 11.25 of the legislation. Pursuant to section 11.09, CSIS is required to apply for judicial authorization to retain a Canadian dataset, within 90 days of its collection.

[111] Second, the AGC states that the uncontradicted affidavit and testimonial evidence in this proceeding is that the only information that will be uploaded into CSIS's holdings is [...] data that is assessed to be threat-related. Consequently, the proposed condition would be duplicative.

[112] In my view, the AGC's submissions do not entirely address the concerns raised by the *Amicus*. As noted above, Affiant 1 was unable to provide a firm date by which incidentally collected [...] data would be destroyed. Nor does section 12 specify any such date.

[113] It bears underscoring that the data in question is [...] data that has been collected from the Devices of individuals who would not be reasonably suspected to be threats to the security of Canada, in the context of the various proposed uses of the Technology in Canada.

[114] In *IMSI*, the short duration of the retention period played a very important role in the Court's conclusion that CSIS could intercept the mobile device identifiers in question without a warrant: *IMSI*, above, at paras 252–254. In this regard, I consider the following observations to be particularly relevant to the present proceeding:

> [254] The retention of third party IMSI or IMEI information beyond a very short period of time, or the analysis of such information for a purpose other than simply assisting to identify the mobile device(s) of a subject of investigation, is not authorized by section 12. For this purpose, a "very short period of time" would be measured in days or weeks, although I will remain open to being persuaded that there are sound reasons for aligning this period with the [...] for the destruction of third party information that is applicable in other contexts, including the retention of certain types of metadata (*X (Re)*, above, at para 253). I expect that this will be the subject of further exchanges with the Attorney General following the release of this decision.

[115] The AGC has not identified a principled basis for adopting a different approach in this case. However, I recognize that some adjustment is warranted in light of Affiant 1's evidence, discussed at paragraph 108 above.

[116] Having regard to that evidence, I consider that an outside period of [...] would not be unreasonable. Nevertheless, consistent with the AGC's representations to the Court in a letter dated June 24, 2022, the Court understands that non-threat-related [...] data will typically be deleted "within days or weeks post-collection." This will occur as soon as CSIS has completed its assessment of the information in question and filed its operational report or the last of its operational reports, in respect of the information. In the exceptional circumstances in which a retention period of [...] is considered to be insufficient, CSIS can always return to the Court to seek an extension of time.

[117] In summary, I agree with the *Amicus* that there should be a limit on how long CSIS may retain incidentally collected [...] data, as defined above. That limit should be [...]. So long as certain additional general operating principles are followed, the incidental collection of [...] data pertaining to non-threat-related parties would not be unreasonable. Those principles are that (i) incidentally collected [...] data will be destroyed as soon as CSIS is able to [...] to its subjects of investigation; (ii) that destruction will occur before any use whatsoever is made of incidentally collected [...] data, and before CSIS ever discovers the identity of the individuals behind that data; (iii) only individuals within CSIS who are authorized users of the technology will have access to incidentally collected [...] data – at present, there are [...] individuals; and, (iv) such [...] data will be sequestered during the assessment period. For greater certainty,

only [...] data that is assessed to be threat-related would be ingested into CSIS's holdings. In the presumably exceptional situation in which CSIS may wish to retain incidentally collected [...] data as a Canadian dataset, it shall not make any use of that data unless and until it receives the approval of the Court pursuant to section 11.13 of the *CSIS Act*. If it failed to bring such an application within 90 days, it would be required to destroy the information pursuant to subsection 11.09(3).

(v) Conclusion

[118] For the reasons provided in parts IV.C. (3)(i)-(iv) above, the manner in which the first proposed use of the Technology within Canada would be carried out would not be unreasonable.

(b) *The Second Proposed Use of the Technology Within Canada*

[119] As with the first of the four proposed uses of the Technology, the second use would be deployed against known targets of CSIS investigations [...] within Canada. However, the objective of this proposed use would be to [...].

[120] The AGC maintains that CSIS could reasonably suspect [...], and therefore deploy the Technology, in two types of situations. The first is where [...]. The example provided was [...]. Given the existence of a nexus to both a target of investigation and threat-related activity, I agree that the reasonable grounds to suspect threshold would be met in this type of situation. That threshold simply requires "something more than a mere suspicion, and something less than a belief based upon reasonable and probable grounds" that the individual in question is *possibly*

engaged in threat-related conduct: *R v Kang-Brown*, 2008 SCC 18, at para 75 [***Kang-Brown***]; and *R v Chehil*, 2013 SCC 49, at para 26 [***Chehil***].

[121] The second type of situation in which the AGC states that this test would be met concerns [...]. In such situations, the AGC states that CSIS could reasonably suspect [...]. Once again, given the existence of a nexus to both a target of investigation and a threat-related event, I agree that the reasonable grounds to suspect threshold would be met in that situation.

[122] I also consider that the cross-checking of collected [...] against the information in CSIS's databases would be permissible in these two types of situations, without a warrant. This is because, in contrast to the first proposed use, this exercise would not be equivalent to a "fishing expedition": see paragraph 93 above. The whole purpose for collecting [...] in CSIS's holdings. This would include presumably lawfully obtained information already [...]. If CSIS were unable to undertake that task, there would be little point in collecting the [...] in question [...].

[123] Turning to the degree of intrusiveness of this second proposed use of the Technology, it is readily apparent that, with one exception, it would not be any more intrusive than the first proposed use, insofar as the privacy interests of individuals whose [...] data is collected are concerned.

[124] The one exception is that CSIS would be able to learn [...]. However, as was the case in *IMSI*, that [...] would remain minimally intrusive in nature: *IMSI*, above, at paras 144, 162–

163, 172, 186 and 247. This is because using the Technology in this way would not enable CSIS to make more than minimal inferences or gain more than minimal insights into the types of lifestyle choices and other private activities that are protected by section 8 of the *Charter*. Indeed, the identities of the individuals behind the collected [...] would remain unknown unless they were already [...] in CSIS's data holdings.

[125] As with the first proposed use of the Technology within Canada, the second proposed use would not enable CSIS to access (i) the content of any communications made with the Devices in question, or (ii) any information stored on or accessible through those Devices.

[126] Likewise, for the same reasons discussed at paragraph 89 above, CSIS would again have a strong "built-in" incentive to minimize the extent to which [...] data of non-threat-related parties would be collected. In this regard, the AGC asserted that measures adopted by CSIS to reduce the risk and scope of such incidental collection would include "[...]." (As with the first proposed use of the Technology, CSIS would [...].)

[127] The *Amicus* agreed that this second proposed use of the Technology would be minimally intrusive, provided that it was subject to the same two conditions that he suggested in respect of the first proposed use, namely: (i) the collected [...] data would not be shared with domestic or foreign agencies; and (ii) incidentally collected data would be deleted as soon as possible, without being uploaded into CSIS's holdings. For the reasons discussed at paragraphs 95-106 above, I do not consider that it would be appropriate to impose the first condition. As to the second condition, and subject to one caveat, I agree that this use of the Technology would only

meet the requirements of section 8 of the *Charter* if incidentally collected data were treated in accordance with the principles described at paragraphs 116-117 above. The caveat is that the [...] CSIS employees who are authorized to utilize the Technology would be permitted to consult an operations-level person when assessing whether [...] collected in this scenario were threat-related. This caveat applies equally to the third scenario discussed immediately below.

[128] I recognize that this second use of the Technology within Canada would enable CSIS to [...] and that in *IMSI* the Court observed that CSIS should not use CSS technology to "geo-locate" anyone without a warrant: *IMSI*, above, at para 5. However, that observation must be understood by reference to the context in which it was made. Specifically, the Court was informed that one of the two uses of CSS technology was to conduct "geo-location operations": *IMSI*, above, at paras 31, 54, 56, 71 and 239. In this regard, the evidence before the Court was that [...] *IMSI*, above, at paras 71 and 156. The Court understood that, being mobile, the device could well be travelling around. The Court was also provided with an explanation of [...] situations in which CSIS had previously conducted such an operation. In that situation, in which CSIS had a warrant, CSIS [...]. These types of situations would constitute [...] which the AGC concedes would require a warrant. The AGC's similar concession in *IMSI* must be understood in the foregoing context: *IMSI*, above, at para 137. In my view, the use of the Technology to [...] would not constitute [...].

(c) *The Third Proposed Use of the Technology within Canada*

[129] The third proposed use of the Technology would be in respect of the same two types of [...] within Canada discussed at paragraphs 120 and 121 above. The principal difference would be that CSIS [...]. The purpose of using the Technology in this third type of situation [...].

[130] Insofar as the initial collection is concerned, the reasonable grounds to suspect set forth in section 12 of the *CSIS Act* would be satisfied [...]. Regarding CSIS's subsequent retention, the reasonable grounds to suspect would be established upon confirmation that the [...] is the same as an [...] already in CSIS's database and linked to [...].

[131] The AGC submits that this proposed use of the Technology would be minimally intrusive for the same reasons as discussed above in relation to the second proposed use. I agree. This assumes that the operational principles and measures discussed at paragraphs 116–117 and 126–127 above are followed and CSIS does not merely [...].

[132] The *Amicus* maintains that this proposed use of the Technology can only be conducted in a way that is minimally intrusive of individuals' rights under section 8 of the *Charter* if it is subject to three conditions. It is unnecessary to discuss the first two here, as they are the same as the conditions the *Amicus* proposed in relation to the first two proposed uses, discussed above.

[133] The third condition proposed by the *Amicus* is that CSIS's third proposed use of the Technology be confined to situations in which CSIS reasonably suspects that [...] in question involves activities within 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 Canada or a foreign state. This language tracks the wording of the third of the four types of threats to the security of Canada defined in section 2 of the *CSIS Act*.

[134] The *Amicus* suggested that the foregoing condition is necessary because this proposed use of the Technology could be used in excessive ways in the absence of [...]. This is particularly so given the "malleability" of CSIS's concept of [...].

[135] In my view, it would not be appropriate to impose this condition on the third proposed use of the Technology. In brief, I do not see any principled basis for limiting this third proposed use of the Technology to only one of the four types of threats to the security of Canada described in section 2 of the *CSIS Act*. Moreover, as a practical matter, such a condition could well create blind spots in CSIS's ability to assess such threats: *Vu*, above, at para 57. [...] are often not easily ascertainable in advance. For essentially the same reason that police are afforded "a certain amount of latitude" with respect to the manner in which they conduct searches (*R v Cornell*, 2010 SCC 31 at paras 22–24), it is appropriate to give CSIS a margin of discretion in determining when [...] exist and when deploying the Technology might assist it to identify [...].

[136] It bears emphasizing that my conclusion regarding CSIS's ability to engage in this proposed use of the Technology without a warrant is premised on CSIS's adherence to the operational principles and measures discussed at paragraphs [116–117 and 126–127] above. It is also based on the AGC's representations that CSIS will not use the Technology to [...] anyone, without a warrant.

(d) *The Fourth Proposed Use of the Technology Within Canada*

(i) Introduction

[137] Whereas the first three proposed uses of the Technology would be entirely within Canada, the fourth proposed use would involve investigative activity both outside and within Canada. In brief, the Technology would [...][5].

[138] In attempting to make this determination, [...]. The AGC underscored that CSIS's collection would be limited to this [...] determination.

[139] In my view, this use of the Technology to [...] would be minimally intrusive. This is so for essentially the same reason that the deployment of the Technology in the second and third proposed uses discussed above would be minimally intrusive. As I have noted, one of the ways in which those proposed uses of the Technology would be intrusive would be by enabling CSIS to obtain [...]. While the capture of this information might ultimately enable CSIS to [...], this alone is minimally intrusive for the reasons discussed at paragraphs 123–-128 and 131. Given that the [...] information obtained in the fourth proposed use would be [...] than in the second and third proposed uses, it would be even more minimally invasive.

[140] It follows that this fourth proposed use of the Technology would not require a warrant.

---

[5] [...]

[141] For greater certainty, the AGC and CSIS have explicitly represented to the Court that as soon as CSIS is able to [...], CSIS would be required to apply for a warrant before making further use of the Technology in relation to [...].

V. Assessment of the Proposed Uses of the Technology Outside Canada (Issue #2)

A. *Introduction*

[142] Outside Canada, CSIS proposes to use the Technology to collect [...] data in two types of situations. The first would be to [...]. These more-than-minimally intrusive investigative activities would all be done outside Canada.

[143] In the second type of situation, CSIS would [...]. As with the first situation described above, this would all be done outside Canada.

[144] In my view, the reasonable grounds to suspect requirement of section 12 of the *CSIS Act* would be satisfied in both of the above-described types of situations.

[145] Accordingly, what remains to be determined is whether section 12 authorizes the degree of intrusiveness of these proposed uses of the Technology, outside Canada, without a warrant. For the reasons that follow, I consider that it does.

[146] I will pause to note for the record that the AGC recognizes that the collection of [...] data outside Canada in the two situations described above could foreseeably result in the incidental or inadvertent collection of [...] data from a Device belonging to a Canadian citizen.

The AGC represented that where CSIS determines that such collection, or indeed any similar collection from a person with a nexus to Canada, has occurred CSIS would sequester the information. The AGC would then return to the Court to make submissions as to whether such incidentally or inadvertently collected information could be collected on a warrantless basis. I agree that the immediate sequestration of such information, combined with an expeditious return to the Court, would be the appropriate manner in which to proceed if and when this type of scenario occurs. For greater certainty, this conclusion is premised on the understanding that CSIS would not make any use of such sequestered information pending further instruction from the Court.

B. *Analysis*

[147] The AGC concedes that the *Charter* applies to CSIS's investigative activities, wherever they occur. In this regard, the AGC notes that the preamble to the *CSIS Act* refers to the importance of CSIS "perform[ing] its duties and functions in accordance with the rule of law and in a manner that respects the [Charter]." Nevertheless, CSIS maintains that foreign nationals with no nexus to Canada have no rights under the *Charter*. Consequently, they cannot have an REP in the [...] data of their Devices, as that concept is understood in the *Charter* jurisprudence.

[148] The *Amicus* acknowledges that foreign nationals with no nexus to Canada do not have rights under section 8 of the *Charter*. Nevertheless, the *Amicus* maintains that those individuals have an REP in the [...] data of their Devices. Given such REP, CSIS would require a warrant to deploy the Technology against those persons in a manner that is more than minimally invasive.

[149] In my view, it is not particularly helpful, or indeed necessary, to focus on whether foreign nationals with no nexus to Canada have an REP in the [...] data of their Devices.

[150] This is because the issue of whether CSIS can engage in the proposed uses of the Technology against such individuals can be determined by answering three different questions. Those are as follows:

1. Do foreign nationals with no nexus to Canada come within the scope of the word "everyone" in section 8 of the *Charter*?

2. Does section 12 authorize investigative activities outside Canada that are more than minimally intrusive, when they are conducted against foreign nationals who have no rights under the *Charter*?

3. Is there any principle of international law that would prevent CSIS from using the Technology abroad against foreign nationals with no nexus to Canada, in the more than minimally intrusive ways that it has proposed?

[151] If the responses to the first and third of these questions is negative and if the response to the second is affirmative, that is the end of the matter. For the reasons discussed below, I find that those are indeed the responses to these three questions. Therefore, CSIS would not require a warrant to deploy the Technology outside Canada in the two specific types of situations described above, and subject to the caveat discussed at paragraph 146 above.

(a) *Do Foreign nationals who have no nexus to Canada come within the scope of section 8 of the Charter?*

[152] Section 8 of the *Charter* states: “Everyone has the right to be secure against unreasonable search or seizure.”

[153] The AGC maintains that the term “everyone” does not extend to foreign nationals who have no nexus to Canada. Consequently, such persons cannot assert rights under the *Charter* in response to Canadian state action. I agree.

[154] The word “everyone” should be interpreted consistently with the manner in which it has been interpreted in connection with other sections of the *Charter*: *R v Lloyd*, 2016 SCC 13, at paras 41–42.

[155] To give the term “everyone” a broader interpretation under section 8 than it has received in those other contexts (e.g., ss. 2, 7, 9, 10 and 12) would have the effect of elevating the rights protected by section 8 over those protected by other sections of the *Charter*. To the extent that this may result in creating a hierarchical approach to *Charter* rights, it is something to be avoided: *Dagenais v Canadian Broadcasting Corp.*, [1994] 3 SCR 835, at 877.

[156] In *Slahi v Canada (Justice)*, 2009 FC 160, at paras 40–48 [***Slahi***], Justice Blanchard relied on certain teachings of the SCC to conclude that the foreign applicants could not engage rights under section 7 of the *Charter*. This was because they had failed to establish a recognized

nexus to Canada. The fact that they were interviewed in Guantanamo Bay by Canadian officials was not considered to be sufficient, in and of itself, to trigger those rights.

[157] In reaching that conclusion, Justice Blanchard reviewed the SCC's jurisprudence dating back to *Singh v Minister of Employment and Immigration*, [1985] 1 SCR 177 [***Singh***], where that Court addressed the issue of whether refugee claimants who are physically present in Canada are entitled to the protection of section 7 of the *Charter*. In the course of providing an affirmative response to that question, Justice Wilson - writing for the majority - stated: "… I am prepared to accept that the term ["everyone"] includes every human being who is physically present in Canada and by virtue of such presence amenable to Canadian law": *Singh*, above, at 202.

[158] After noting that statement in *Singh*, Justice Blanchard quoted a passage from Justice L'Heureux-Dubé's dissenting reasons in *R v Cook*, [1998] 2 SCR 597 [***Cook***]. That passage included the following observation:

> The appellant is claiming rights under s. 10(b), which guarantees its protections to "everyone". The term "everyone" seems quite broad. Nevertheless, interpreting it must take into account the purposes of the *Charter*. I am not convinced that passage of the *Charter* necessarily gave rights to everyone in the world, of every nationality, wherever they may be, even if certain rights contain the word "everyone". Rather, I think that it is arguable that "everyone" was used to distinguish the rights granted to everyone on the territory of Canada from those granted only to citizens of Canada and those granted to persons charged with an offence.

Cook, above, at para 86, quoted in *Slahi*, above, at para 43.

[159] I pause to observe that the majority in *Cook* was not persuaded by a similar line of reasoning advanced by the AGC, who intervened in the proceedings. However, in concluding that section 10(b) of the *Charter* applied to Canadian detectives who interviewed the appellant (a U.S. citizen) in the U.S., the majority stressed the particular facts in that case. Those particular facts included that the appellant was being investigated for a murder committed in Canada, which would be prosecuted in this country. In that context, the majority observed that the appellant "was being compulsorily brought before the Canadian justice system": *Cook*, above, at para 53. This appears to have provided the principal basis for their finding that he ought to have been properly advised of his right to counsel, as required by section 10(b) of the *Charter*. The majority added: "This situation is far different from the myriad of circumstances in which persons outside Canada are trying to claim the benefits of the Charter simpliciter": *Cook*, above, at para 53.

[160] Subsequently, in *R v Hape*, 2007 SCC 26, at paras 83–93 [***Hape***], the SCC determined that the majority decision in *Cook* put the focus in the wrong place, and that this gave rise to various problems. Those problems included practical and theoretical difficulties that arise when the majority's approach "is applied to different facts (*such as a search and seizure*)": *Hape*, above, at para 83 [emphasis added]. For the present purposes, I agree with the AGC that it is unnecessary to delve further into the analysis in *Hape*. This is because it focused on the application of the *Charter* to a search and seizure of a Canadian businessman's investment company in Turks and Caicos by Canadian police officers who were operating there under the authority of a senior local police official. In the case at bar, it will suffice to note that the majority opinion in *Hape* effectively overturned the majority decision in *Cook*, and in the course

of doing so, mentioned Justice L'Heureux-Dubé's dissenting view in *Cook*: *Hape*, above, at para 81. The Court did not further comment upon that view, other than to note that it was concurred in by Justice McLachlin (as she then was).

[161] Returning to *Slahi*, after quoting Justice L'Heureux-Dubé's dissenting view in *Cook*, Justice Blanchard proceeded to briefly discuss two other decisions of the SCC. The first was *Canada (Justice) v Khadr*, 2008 SCC 28, at para 31, where the SCC held that "s. 7 imposes a duty on Canada to provide disclosure of materials in its possession arising from its participation in the foreign process that is contrary to international law and jeopardizes the liberty of a Canadian citizen." [Emphasis added by the Court in *Slahi*, above, at para 45.] In the second decision, *R v Harrer*, [1995] 3 SCR 562, at para 11, Justice LaForest, writing for the majority, observed:

> Subject to whatever argument may be made to the contrary, it strikes me that the automatic exclusion of *Charter* application outside Canada might unduly restrict the protection Canadians have a right to expect against the interference with their rights by our governments or their agents.

[Emphasis added by the Court in *Slahi*, above, at para 46.]

[162] Having regard to the foregoing jurisprudence, the Court in *Slahi* concluded:

> [47] In summary, the jurisprudence of the Supreme Court teaches that section 7 *Charter* protections may be available to non-Canadians when they are physically present in Canada or subject to a criminal trial in Canada, and that Canadian citizens, in certain circumstances, may assert their section 7 *Charter* rights when they are outside Canada …
>
> [48] The Applicants here have failed to establish a nexus to Canada that would engage their section 7

> *Charter* rights as they relate to the Guantanamo Bay interviews. It must be remembered that the *Charter*, an integral part of Canada's supreme law, is a Canadian instrument enacted to enshrine and protect the fundamental rights of Canadians and those finding themselves within Canada's territory. Its extraterritorial reach is exceptional and limited, as is mandated by respect for the principles of sovereignty and judicial comity. This Court is not prepared to extend the *Charter*'s reach beyond that which has already been decided. The Applicants are not Canadian citizens. They have failed to establish the required connection to Canada. Consequently, their circumstances cannot engage a section 7 *Charter* right.

[Emphasis added.]

[163] On appeal to the FCA, Justice Blanchard's conclusion was upheld: *Slahi v Canada (Justice)*, 2009 FCA 259. There, the FCA stated as follows:

> [4] The only issue to be decided in these consolidated appeals is whether the Applications Judge erred in concluding that section 7 was inapplicable to the appellants while detained by the U.S. authorities at Guantánamo Bay because they are not Canadian citizens. Substantially for the reasons given by the Applications Judge, we are of the view that his conclusion was correct. *Khadr* is distinguishable on the ground that Mr Khadr is a Canadian citizen, whereas the appellants are not. Further, there are no proceedings pending in Canada against the appellants which might provide a nexus to Canada.

[164] Leave to further appeal to the SCC was dismissed: *Slahi v Canada (Justice)*, 2009 FCA 259, leave to appeal to SCC refused, 33409 (18 February 2010).

[165] Justice Blanchard's reasoning in *Slahi* was also endorsed in *obiter dictum* remarks by Justice Rennie (as he then was) in *Tabingo v Canada (Citizenship and Immigration)*, 2013 FC 377 [***Tabingo***]. There, the foreign applicants for judicial review alleged breaches of sections 7 and 15 of the *Charter*. Given that the respondent did not dispute either the applicants' standing or the application of the *Charter*, Justice Rennie refrained from explicitly ruling on the issue of whether they were entitled to the protection of the *Charter*. However, he expressed reservations as to the correctness of the respondent's concession: *Tabingo*, above, at para 79. In the course of doing so, he made the following observation:

> [65] There has been clear guidance from the Supreme Court of Canada and the Federal Court of Appeal as to when the *Charter* applies to the actions of Canadian officials outside of Canada. […] The weight of the case law indicates that non-citizens outside of Canada may not claim the protection of the *Charter*, absent exceptional circumstances involving the actions of Canadian officials or agents abroad.

[166] The guidance to which Justice Rennie was referring was the jurisprudence that Justice Blanchard discussed in *Slahi*, as well as this Court's decision in *Amnesty International Canada v Canada (Chief of the Defence Staff)*, 2008 FC 336 [***Amnesty International***] (aff'd 2008 FCA 401 at para 36). The latter case involved detainees held by the Canadian Forces in Afghanistan in the context of an ongoing armed conflict. There, Justice Mactavish (as she then was) concluded that while the detainees were protected by international humanitarian law, they did not have rights under sections 7, 10, or 12 of the *Charter*. This was because the Government of Afghanistan had not consented to the application of Canadian laws, including the *Charter*, to its citizens, within its territory: *Amnesty International*, above, at paras 171–172.

[167] Justice Rennie further observed in *Tabingo* that the foregoing jurisprudence was consistent with other jurisprudence of the FCA and this Court. In this regard he stated as follows:

> [75] Other recent decisions of this Court have found that non-citizens outside of Canada generally do not hold *Charter* rights: *Zeng v Canada (Attorney General)*, 2013 FC 104, paras 70-72; *Kinsel v Canada (Minister of Citizenship and Immigration)*, 2012 FC 1515, paras 45-47; *Toronto Coalition to Stop the War v Canada (Minister of Public Safety and Emergency Preparedness)*, 2010 FC 957, paras 81-82. <u>These three decisions followed Justice Blanchard's determination that a *Charter* claim may only be advanced by an individual who is present in Canada, subject to criminal proceedings in Canada, or possessing Canadian citizenship.</u>
>
> [76] This limitation on the application of the *Charter* is not a recent development. Even prior to *Slahi*, the Federal Court and the Federal Court of Appeal had interpreted *Singh* as barring *Charter* claims from non-citizens outside Canada: *Canadian Council of Churches v Canada (Minister of Employment and Immigration)*, [1990] 2 FC 534 (CA) (aff'd on other grounds [1992] 1 SCR 236); *Ruparel v Canada (Minister of Employment and Immigration)*, [1990] 3 FC 615; *Lee v Canada (Minister of Citizenship and Immigration)*, [1997] FCJ No 242; *Deol v Canada (Minister of Citizenship and Immigration)*, [2001] FCJ No 1034 (aff'd on other grounds 2002 FCA 271).

[Emphasis added.]

[168] Ultimately, Justice Rennie dismissed the applicants' *Charter* claims on their merits. His reasoning and conclusions in that regard were upheld by the FCA: *Tabingo v Canada (Citizenship and Immigration)*, 2014 FCA 191, at para 96, leave to appeal to the SCC refused, 36213 (30 April 2015).

[169] The reservations expressed by Justice Rennie regarding the issue of the application of the *Charter* to the foreign applicants in *Tabingo* were shared by Justice Gleason (as she then was) in *Jia v Canada (Citizenship and Immigration)*, 2014 FC 596, at paras 108–110. However, consistent with Justice Rennie's approach, Justice Gleason refrained from ruling on this issue because she was able to dismiss the applicant's claims under sections 7 and 15 of the *Charter* on their merits.

[170] In summary, in light of the jurisprudence discussed above (including the cases referenced in the quotes from *Tabingo*), I agree with the AGC that foreign nationals who do not have one of the three recognized grounds of nexus to Canada summarized immediately below do not come within the scope of the term "everyone" in section 8 of the *Charter*. In other words, the interpretations that have been given to the term "everyone", as it appears in sections 2, 7, 10(b) and 12 of the *Charter*, and to the words "every individual" in section 15, apply equally to section 8. Consequently, foreign nationals who have no recognized nexus to Canada have no rights under section 8 of the *Charter*. The first question listed in paragraph 150 above is therefore answered in the negative.

[171] As noted in *Tabingo*, above, at paragraph 75, the three recognized categories of nexus are (i) Canadian citizenship, (ii) physical presence in Canada, and (iii) being subject to criminal proceedings in Canada.

[172] For greater certainty, the AGC has acknowledged that as soon as CSIS is able to confirm that [...] would have the requisite nexus to Canada. In such circumstances, the AGC and CSIS

have explicitly represented to the Court that CSIS would be required to apply for a warrant before making further use of the Technology against those individuals.

(b) *Does section 12 authorize investigative activities outside Canada that are more than minimally intrusive, when they are conducted against foreign nationals who have no rights under the Charter?*

[173] My conclusion regarding the scope of the protections afforded by section 8 of the *Charter* does not provide a sufficient basis upon which to determine whether CSIS can engage in the proposed uses of the Technology outside Canada, without a warrant. To answer this question, it is necessary to determine whether those activities are authorized by law.

[174] In the present context, the relevant law is section 12 of the *CSIS Act*. Consequently, the question for the Court is whether section 12 authorizes CSIS to engage in more than minimally intrusive activities outside Canada, against foreign nationals with no nexus to Canada.

[175] Subsection 12(2) explicitly authorizes CSIS to "perform its duties and functions under subsection (1) within or outside Canada."

[176] This Court has consistently held that, without a warrant, section 12 only authorizes CSIS to engage in activities that are minimally intrusive. However, that jurisprudence involved subjects of investigation who benefitted from the rights afforded by section 8 of the *Charter*.

[177] Where CSIS's subjects of investigation do not have those rights, this limitation on the powers conferred by section 12 falls away. This is consistent with the following observation in *X (Re)*, 2014 FCA 249, at para 82 [***X (Re) FCA***]:

> … [S]ection 12 does not give CSIS an exemption from the operation of the laws of general application. Thus, when intrusive methods are resorted to, <u>which methods would otherwise constitute a crime or a breach of the *Charter* guarantee against unreasonable search and seizure</u>, the Service may apply to the Federal Court for the issuance of a warrant under section 21 of the CSIS Act.
>
> [Emphasis added.]

[178] I recognize that "prior authorization, usually in the form of a valid warrant, has been a consistent prerequisite for a valid search and seizure both at common law and under most statutes": *Hunter*, above, at 160. However, section 12 overrides the common law by providing specific authority to CSIS to collect, 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.

[179] The foregoing interpretation of the scope of CSIS's powers in respect of foreign nationals who do not have a nexus to Canada is supported by the legislative history of section 12. Specifically, when the Standing Committee on Public Safety and National Security was considering Bill C-44, Green Party leader and Member of Parliament Elizabeth May proposed the following amendment to Bill C-44, which was supported by the New Democratic Party, as the official opposition:

> The proposal is to have a stand-alone section that will be inserted right after proposed subsection 21(3.1). As you can see, it would be within clause 8:
>
> (3.2) For greater certainty, a warrant under this section is required for any investigation outside of Canada that
>
> (a) involves an investigative activity that, were it conducted inside Canada, would require a warrant by reason of the *Canadian Charter of Rights and Freedoms*...
>
> …This will clarify ambiguities. It will ensure that our actions are consistent with the *Charter of Rights and Freedoms* when occurring overseas.

[180] This amendment was not adopted: House of Commons, *Standing Committee on Public Safety and National Security*, 2-41, No 42 (1 December 2014) at 12. This suggests that Parliament did not intend that CSIS would require a warrant whenever engaging in activities outside Canada that would require a warrant in Canada, by reason of section 8 of the *Charter*: *Tele-Mobile Co. v Ontario*, 2008 SCC 12, at para 42; *Canada (Information Commissioner) v Canada (Minister of National Defence)*, 2011 SCC 25, at para 27; and *Reference re Broadcasting Regulatory Policy CRTC 2010-167 and Broadcasting Order CRTC 2010-168*, 2012 SCC 68, at para 73.

[181] I consider it relevant to add that, when Bill C-44 was subsequently considered by the Standing Senate Committee on National Security and Defence, CSIS's Director of the day, Mr. Michel Coulombe, was asked by Senator Olsen what activities outside Canada would require a warrant. Mr. Coulombe replied: "At the moment, it would be the same type of activities that require a warrant in Canada. So when there is a breach of section 8 of the *Charter*, we require

warrants": Senate, *Senate Standing Committee on National Security and Defence*, 2-41, No 14 (9 March 2015), at 115.

[182] In summary, in the absence of any requirement for CSIS to obtain prior judicial authorization, whether under the *Charter* or otherwise, before engaging in the intrusive uses of the Technology described at paragraphs 142-143 above, such investigative activities would not require a warrant. That is to say, CSIS would not require a warrant to deploy the Technology outside Canada in the manner that it has proposed. This interpretation of CSIS's authority under section 12 of the *CSIS Act* is consistent with the legislative history discussed above.

[183] Accordingly, the second question listed in paragraph 150 above is answered in the affirmative.

> (c) *Is there any principle of international law that would prevent CSIS from using the Technology abroad against foreign nationals with no nexus to Canada, in the more than minimally intrusive ways that it has proposed?*

[184] The *Amicus* expressed a concern that the foregoing interpretation of section 12 would be tantamount to giving CSIS "a blank cheque in regard to searches of foreign nationals." I disagree.

[185] The *Amicus* did not produce anything before the Court to suggest that the warrantless uses of the Technology proposed by CSIS in this proceeding would contravene or otherwise offend international law.

[186] Relying on the following authorities, the *Amicus* acknowledged that espionage, *per se*, is not contrary to international law: *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press: 2017), at 169; C. Forcese, "Pragmatism and Principle: Intelligence Agencies and International Law" (2016) 102 Va L Rev 67 at 71–72. I agree. The issue of whether such activity contravenes international law ought to be determined on the specific facts of each case.

[187] On the specific facts of this case, and in the absence of any evidence to the contrary, I conclude that there is no principle of international law that would prevent CSIS from using the Technology abroad against foreign nationals with no nexus to Canada, in the more than minimally intrusive ways that it has proposed. Contrary to the *Amicus*' suggestion, this does not give CSIS a "blank cheque in regard to searches of foreign nationals." Among other things, CSIS would remain subject to the limitations of section 12, including the "reasonable grounds to suspect" and "strictly necessary" requirements. In addition, the *CSIS Act* contains accountability measures that ensure oversight of CSIS's activities under section 12: see generally *IMSI*, at paras 230-235.

[188] Moreover, as recognized by the AGC, CSIS cannot collect information outside Canada in a manner that would be contrary to its legal obligations under the *Avoiding Complicity in Mistreatment by Foreign Entities Act* SC 2019, c 13, s 49.1 and the *Directions for Avoiding Complicity in Mistreatment by Foreign Entities (Director of the Canadian Security Intelligence Service)*, 2019-1302 (Directions).

[189] More broadly, any information collected by CSIS outside Canada and intended to be used in a criminal proceeding would be subject to the *Charter* requirements for admissibility at trial.

[190] I also agree with the *Amicus* that, for the purposes of the present proceeding, section 12 of the *CSIS Act* is subject to the presumption of conformity with international law: *Canada (Minister of Citizenship and Immigration) v Vavilov*, 2019 SCC 65, at paras 114 and 182. This is because section 12 does not include the type of language that appears in subsections 21(3) and section (24) ("notwithstanding any other law") and in subsections 21(3.1) and (4) ("despite any other law").

[191] Finally, it appears to be common ground between the *Amicus* and the AGC that the principle of conformity with international law would prevent section 12 from being interpreted in a manner that might authorize torture or similar violations of international human rights law. Beyond that, it is relevant to note that the *Amicus* did not wish to speculate regarding the extent to which international law might constrain the authority provided under section 12 of the *CSIS Act*.

[192] In summary, for the purposes of the present proceeding, and in the absence of any evidence or persuasive argument to the contrary, I find that that CSIS's proposed uses of the Technology outside Canada would not contravene any principle of international law. Therefore, the third question listed at paragraph 150 above is answered in the negative.

[193] I will add in passing that I take some comfort from the fact that the FCA has rejected the proposition that "intrusive investigative measures conducted abroad would necessarily violate international law or the principle of comity between nations": *X (Re) FCA*, above, at para 80. Although the FCA proceeded to find that CSIS requires a warrant whenever its methods of investigation are intrusive, it added the important qualification that this applied to methods "that would otherwise constitute a crime or breach of the *Charter* guarantee against unreasonable search and seizure": *X (Re) FCA*, above, at paras 81–82. I will simply add that in that case, the subjects of investigation in that case were Canadian citizens who were outside Canada, and not—as is the case here—foreign nationals with no nexus to Canada: see *X (Re) FCA*, above, at paras 9 and 11.

VI. **Conclusion**

[194] For the reasons provided in parts IV.C. 3 (a) – (d) above, the four proposed uses of the Technology within Canada that CSIS has proposed would not require a warrant.

[195] It bears emphasizing that my conclusion regarding CSIS's ability to engage in these proposed uses of the Technology without a warrant is premised on CSIS's adherence to the operational principles and measures discussed at paragraphs 62, 88, 116–117, 126–127 and 141 above. It is also based on the AGC's representations that only [...] data that is assessed to be threat-related would be ingested into CSIS's holdings, and that CSIS will not use the Technology [...] who has a recognized nexus to Canada, without a warrant.

[196] For the reasons provided in Part V above, CSIS proposed uses of the Technology outside Canada, against foreign nationals with no nexus to Canada, would also not require a warrant.

JUDGMENT in CSIS-1-21

THIS COURT'S JUDGMENT is that:

1. The Technology may be deployed within Canada in the four specific ways that CSIS has proposed, without a warrant, provided that such uses of the Technology are consistent with the reasons provided above, and in particular with paragraphs 62, 88, 116-117, 126-127 and 141.

2. The Technology may be deployed outside Canada against foreign nationals with no nexus to Canada, without a warrant, in the two types of situations described at paragraphs 142 and 143 of the reasons above.

"Paul S. Crampton"
Chief Justice

Confidential Appendix I – The Technology

Appendix I as referred to in paragraph 7 of this Judgment and Reasons is comprised of 14 pages and is fully redacted.

Appendix II – Relevant Legislation

***Canadian Security Intelligence Service Act*, RSC 1985, c C-23**	***Loi sur le service canadien du renseignement de sécurité*, LRC 1985, c C-23**
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 Government of Canada.	**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 Canada et le conseille à cet égard.
No territorial limit	**Aucune limite territoriale**
(2) For greater certainty, the Service may perform its duties and functions under subsection (1) within or outside Canada. R.S., 1985, c. C-23, s. 12, 2015, c. 9, s. 3	**(2)** Il est entendu que le Service peut exercer les fonctions que le paragraphe (1) lui confère même à l'extérieur du Canada. L.R. (1985), ch. C-23, art. 12 2015, ch. 9, art. 3
Measures to reduce threats to the security of Canada	**Mesures pour réduire les menaces envers la sécurité du Canada**
12.1 (1) If there are reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada, the Service may take measures, within or outside Canada, to reduce the threat.	**12.1 (1)** S'il existe des motifs raisonnables de croire qu'une activité donnée constitue une menace envers la sécurité du Canada, le Service peut prendre des mesures, même à l'extérieur du Canada, pour réduire la menace.

Limits

(2) The measures shall be reasonable and proportional in the circumstances, having regard to the nature of the threat, the nature of the measures, the reasonable availability of other means to reduce the threat and the reasonably foreseeable effects on third parties, including on their right to privacy.

Alternatives

(3) Before taking measures under subsection (1), the Service shall consult, as appropriate, with other federal departments or agencies as to whether they are in a position to reduce the threat

Canadian Charter of Rights and Freedoms

(3.1) The Canadian Charter of Rights and Freedoms is part of the supreme law of Canada and all measures taken by the Service under subsection (1) shall comply with it

Warrant — Canadian Charter of Rights and Freedoms

(3.2) The Service may take measures under subsection (1) that would limit a right or freedom guaranteed by the Canadian Charter of Rights and Freedoms only if a judge, on an application made under section 21.1, issues a

Limites

(2) Les mesures doivent être justes et adaptées aux circonstances, compte tenu de la nature de la menace et des mesures, des solutions de rechange acceptables pour réduire la menace et des conséquences raisonnablement prévisibles sur les tierces parties, notamment sur leur droit à la vie privée.

Autres options

(3) Avant de prendre des mesures en vertu du paragraphe (1), le Service consulte, au besoin, d'autres ministères ou organismes fédéraux afin d'établir s'ils sont en mesure de réduire la menace.

Charte canadienne des droits et libertés

(3.1) La Charte canadienne des droits et libertés fait partie de la loi suprême du Canada et toutes les mesures prises par le Service en vertu du paragraphe (1) s'y conforment.

Mandat — Charte canadienne des droits et libertés

(3.2) Le Service ne peut, en vertu du paragraphe (1), prendre des mesures qui limiteraient un droit ou une liberté garanti par la Charte canadienne des droits et libertés que si, sur demande présentée au titre de l'article

warrant authorizing the taking of those measures.

21.1, un juge décerne un mandat autorisant la prise de ces mesures.

Condition for issuance

(3.3) The judge may issue the warrant referred to in subsection (3.2) only if he or she is satisfied that the measures, as authorized by the warrant, comply with the Canadian Charter of Rights and Freedoms.

Condition

3.3) Le juge ne peut décerner le mandat visé au paragraphe (3.2) que s'il est convaincu que les mesures, telles qu'autorisées par le mandat, sont conformes à la Charte canadienne des droits et libertés.

Warrant — Canadian law

(3.4) The Service may take measures under subsection (1) that would otherwise be contrary to Canadian law only if the measures have been authorized by a warrant issued under section 21.1.

Mandat — droit canadien

(3.4) Le Service ne peut, en vertu du paragraphe (1), prendre des mesures qui seraient par ailleurs contraires au droit canadien que si ces mesures ont été autorisées par un mandat décerné au titre de l'article 21.1.

Notification of Review Agency

(3.5) The Service shall, after taking measures under subsection (1), notify the Review Agency of the measures as soon as the circumstances permit.

Avis à l'Office de surveillance

(3.5) Dans les plus brefs délais possible après la prise de mesures en vertu du paragraphe (1), le Service avise l'Office de surveillance de ces mesures.

Clarification

(4) For greater certainty, nothing in subsection (1) confers on the Service any law enforcement power. 2015, c. 20, s. 42, 2019, c. 13, s. 23, 2019, c. 13, s. 98

Précision

(4) Il est entendu que le paragraphe (1) ne confère au Service aucun pouvoir de contrôle d'application de la loi. 2015, ch. 20, art. 42, 2019, ch. 13, art. 23, 2019, ch. 13, art. 98

Prohibited conduct

Interdictions

12.2 (1) In taking measures to reduce a threat to the security of Canada, the Service shall not	**12.2 (1)** Dans le cadre des mesures qu'il prend pour réduire une menace envers la sécurité du Canada, le Service ne peut :
(a) cause, intentionally or by criminal negligence, death or bodily harm to an individual;	**a)** causer, volontairement ou par négligence criminelle, des lésions corporelles à un individu ou la mort de celui-ci;
(b) wilfully attempt in any manner to obstruct, pervert or defeat the course of justice;	**b)** tenter volontairement de quelque manière d'entraver, de détourner ou de contrecarrer le cours de la justice;
(c) violate the sexual integrity of an individual;	**c)** porter atteinte à l'intégrité sexuelle d'un individu
(d) subject an individual to torture or cruel, inhuman or degrading treatment or punishment, within the meaning of the Convention Against Torture;	**d)** soumettre un individu à la torture ou à d'autres peines ou traitements cruels, inhumains ou dégradants, au sens de la Convention contre la torture;
(e) detain an individual; o	**e)** détenir un individu;
(f) cause the loss of, or any serious damage to, any property if doing so would endanger the safety of an individual.	**f)** causer la perte de biens ou des dommages importants à ceux-ci si cela porterait atteinte à la sécurité d'un individu.
2) [Repealed, 2019, c. 13, s. 99], 2015, c. 20, s. 42, ,2019, c. 13, s. 99	**(2)** [Abrogé, 2019, ch. 13, art. 99], 2015, ch. 20, art. 42, 2019, ch. 13, art. 99
***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**	***Charte canadienne des droits et libertés*, partie I de la *Loi constitutionnelle* de 1982, édictée comme l'annexe B de la *Loi de 1982 sur le Canada, 1982*, c 11 (R.-U.)**

Search or seizure	**Fouilles, perquisitions ou saisies**
8 Everyone has the right to be secure against unreasonable search or seizure.	**8** Chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives

FEDERAL COURT

SOLICITORS OF RECORD

DOCKET:	CSIS 1-21
STYLE OF CAUSE:	IN THE MATTER OF AN APPLICATION BY [...] FOR WARRANTS PURSUANT TO SECTIONS 12 AND 21 OF THE *CANADIAN SECURITY INTELLIGENCE SERVICE ACT*, RSC 1985, c C-23 AND IN THE MATTER OF [...] THREAT-RELATED ACTIVITIES
PLACE OF HEARINGS:	OTTAWA, ONTARIO
DATES OF HEARINGS:	JANUARY 25, 2022 FEBRURARY 9 & 10, 2022 MARCH 23, 2022
JUDGMENT AND REASONS:	CRAMPTON C.J.
DATED:	OCTOBER 21, 2022

APPEARANCES:

Amy Joslin-Besner Jeffrey Johnston Jay Pelletier	FOR THE APPLICANT THE ATTORNEY GENERAL OF CANADA
Gib van Ert	*AMICUS CURIAE*

SOLICITORS OF RECORD:

The Attorney General of Canada	FOR THE APPLICANT
Gib van Ert	*AMICUS CURIAE*