Federal Court Cour fédérale

~~**TOP SECRET**~~

Date: 20220309

Docket: [redacted]

Citation: 2020 FC 697

Ottawa, Ontario, March 09, 2022

PRESENT: The Honourable Mr. Justice O'Reilly

BETWEEN:

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

AND IN THE MATTER OF [A FOREIGN STATE, GROUP OF STATES, CORPORATION, OR PERSON]

AMENDED JUDGMENT AND REASONS

TABLE OF CONTENTS

I. Background 2
II. Issue One – What is the scope of s 16 of the *CSIS Act*? 5
A. Background – The History and Purpose of s 16 6
B. Incidental Collection of Information About Canadians 8
(1) Introduction 8
(2) Background 9
(3) The Service's practices relating to information about Canadians 11
(4) Communications and privileges of elected officials 18
C. The Relationship Between s 16 and s 12 27
D. Proposed Changes to the s 16 Warrant Templates 33
(1) Incidental changes to warrant templates 34
(2) Clarifying the scope of some powers 35

(3) New powers or locations 36
(4) Conclusion on warrant templates 37
III. Issue Two – Does s 16 authorize use of CSS technology? 37
IV. Issue Three – Does s 16 authorize interception of [redacted] data? 45
(1) The Technology 46
(2) Does s 16 provide sufficient legal authority? 51
V. Issue Four – Does s 16 authorize interception of communications outside Canada? 59
VI. Conclusion and Disposition 62

I. Background

[1] This case began as an application for warrants to gather foreign intelligence pursuant to s 16 of the *Canadian Security Intelligence Act*, RSC 1985, c 23 (see Annex for all provisions cited). It then grew, becoming a vehicle for the consideration of a number of issues that have arisen in the context of s 16 over recent years.

[2] Section 16 grants the Service authority to provide assistance to the Minister of National Defence or the Minister of Foreign Affairs by collecting information or intelligence about the capabilities, intentions, or activities of a foreign state or foreign person. The Service's role under s 16 is distinct from its primary mandate to investigate threats to the security of Canada under s 12 of the *CSIS Act*.

[3] The original application before me was heard in October 2017. Counsel for the Attorney General of Canada had alerted the Court that the application would include submissions on amendments that the Service was seeking to the templates on which s 16 warrants were then based, as well as representations on the treatment of information collected about Canadians,

including elected officials, in the course of s 16 investigations. The latter was in response to an earlier Direction from the Court requesting the Service to explain its practices and procedure in a future s 16 warrant application. (I provide further details relating to that Direction below.)

[4] After the October 2017 hearing, I appointed two *amici curiae* to assist me, Mr. Gordon Cameron and Mr. Owen Rees. (Mr. Rees withdrew as *amicus* in the fall of 2018 due to a change in his employment). In March 2018, the AGC sought to address other issues that had not been previously considered by the Court in the s 16 context. In addition to the issues relating to the warrant templates and the treatment of information about Canadians, the AGC, jointly with the *amici*, requested that I address:

- The interplay between s 12 of the CSIS Act and s 16 (this was in response to concerns expressed periodically by the Court).

- Whether s 16 gives lawful authority for the Service to employ cell-site simulator (CSS) technology.

- Whether s 16 gives lawful authority for the Service to conduct [redacted] surveys.

- Whether s 16 gives lawful authority for the Service to intercept communications of [foreign persons] when they are travelling outside of Canada.

[5] Shortly thereafter, the AGC filed a number of additional affidavits relating to these issues. A schedule was worked out for the presentation of evidence and oral arguments.

A hearing took place in July 2018 and supplementary written submissions were received up until December 2018.

[6] While I have addressed all of the issues presented to me, I should point out that in some areas this judgment is simply a summary of information I received about the Service's s 16 activities that do not require a definitive ruling. For example, in terms of the Service's policies and practices on collecting and retaining information about Canadians, I describe those matters in detail and note the shortcomings that the *amici* identified. But I did not have a legal basis on which to order the Service to do more. I do, however, point out areas where the Service's policies and practices should be bolstered. Similarly, I describe how the Service carries out parallel operations under sections 12 and 16 and note some concerns about them but, again, found no legal basis for an Order.

[7] However, three areas did require rulings – the proposed use of CSS technology, the collection of [redacted] data, and the interception of [foreign persons'] communications outside Canada.

[8] I have consolidated the various issues before me under these four headings:

i. What is the scope of s 16 of the *CSIS Act* (particularly as it relates to the collection of information about Canadians and to concurrent investigations of threats to the security of Canada under s 12, and the appropriate warrant templates for the execution of intrusive powers in the collection of foreign intelligence)?

ii. Does s 16 authorize use of CSS technology?

iii. Does s 16 authorize interception of [redacted] data?

iv. Does s 16 authorize interception of [foreign persons'] communications outside Canada?

[9] In sum, I find that the Service's treatment of information about Canadians, including elected officials is satisfactory, but should be improved. I also conclude that the Service's approach to parallel investigations pursuant to ss 12 and 16 is satisfactory. I have also found that s 16 provides sufficient legal authority to the Service to use CSS technology. However, I find that s 16 does not provide lawful authority to the Service to intercept [redacted] data; a warrant is required to do so. Finally, I conclude that s 16 authorizes the interception, within Canada, of a [foreign person's] communications while outside Canada.

II. Issue One – What is the scope of s 16 of the *CSIS Act*?

[10] This application requires me to consider the overall scope of s 16 against which some of the more specific questions set out above can be posed. In this section, I begin with some background, then I will discuss the issue of the incidental collection of information about Canadians, including elected officials, in the conduct of s 16 investigations. I will also compare and contrast s 16 with s 12 and discuss the changes that the Service proposes to make to the s 16 warrant templates, largely to bring s 16 warrants into line with s 12 warrants.

A. *Background – The History and Purpose of s 16*

[11] From the beginning – that is, when the *CSIS Act* was enacted in 1984 – the Service was given the express authority, within Canada, to assist the Minister of National Defence and the Minister of Foreign Affairs in gathering information about the "capabilities, intentions or activities" of foreign states or any persons other than Canadian citizens, permanent residents, or corporations (s 16(1)(*a*),(*b*)). In this decision, I will refer to this mandate as the Service's role in gathering "foreign intelligence."

[12] It was also clear, however, that the need for the Service to be involved in protecting Canada from foreign clandestine activities was merely a secondary role (or even a tertiary one, according to the Special Committee on the Security Intelligence Service, *Report of the Special Committee of the Senate on the Canadian Security Intelligence Service: Delicate Balance: A Security Intelligence Service in a Democratic Society* (Ottawa: Senate of Canada), at para 49). See also *Re X*, 2018 FC 738 at para 28; *Re X (Associated Data)* 2016 FC 1105 at para 165.

[13] Nevertheless, s 16 provides broad powers. Arguably, the terms "capabilities, intentions or activities" could refer to virtually anything a foreign country [or foreign person] might wish to learn, achieve, obtain, accomplish, or carry out. Further, in pursuit of its s 16 mandate, the Service can request the Court to grant it a range of intrusive powers, including search, seizure, and electronic surveillance, to collect intelligence relating to any of those objects in order to assist one or both of the named Ministers.

[14] The range of matters on which a Minister might seek assistance is also broad. The mandate of the Minister of Foreign Affairs, for example, includes conducting the external affairs of Canada, as well as international trade, commerce, and development. Global Affairs Canada identifies current priorities as including a comprehensive engagement with countries in the Asia-Pacific Region, as well as diversified international trade and foreign investment. Other notable priorities include combatting drug trafficking, maintaining constructive relations with the United States, and expanding Canadian leadership on the global scene in areas such as human rights, climate change, and peacekeeping. The Minister also has responsibility for Canada's diplomatic relations, which includes ensuring that foreign diplomats and consular agents in Canada abide by their obligations not to violate Canadian laws or interfere in Canada's internal affairs.

[15] It is perhaps not surprising that the Service scoops up vast quantities of foreign intelligence when it exercises the broad mandate and authority given to it by Parliament under s 16.

[16] At the same time, it is important to recognize that the Service's s 16 mandate contains limits. Its authority to collect foreign intelligence has always been strictly confined to foreign entities, and has precluded the targeting of Canadians. Section 16 allows the Service, within Canada, to gather information or intelligence about a foreign state or group of foreign states, or of a person who is not a Canadian citizen, permanent resident of Canada, or a Canadian corporation. It specifically provides that the Service's assistance cannot be directed at Canadians, whether citizens, permanent residents, or companies (see *Re CSIS*, 2012 FC 1437 at para 98, per

Justice Anne Mactavish, now a justice of the Federal Court of Appeal). This means that the Service can intercept communications of Canadians under s 16 only incidentally. These incidental interceptions are an inevitable by-product of the collection of foreign intelligence, especially when powers of electronic surveillance are employed.

[17] The Service has an overarching duty to minimize intrusions on the privacy of Canadians who are innocent third parties to a s 16 investigation. Accordingly, the Court requires the Service to provide in advance the names of persons whose communications may be incidentally intercepted (pursuant to *R v Chesson*, [1988] 2 SCR 148). Where appropriate, the Court can impose terms or conditions on the execution of a s 16 warrant to curtail excessive intrusions on privacy. However, intrusions on the privacy of targets are significantly greater than intrusions on the privacy of third parties because, unlike targets, their communications cannot be intercepted intentionally (*Re CSIS* at paras 33-34).

B. *Incidental Collection of Information About Canadians*

(1) Introduction

[18] The fact that incidental collection of communications by, and information about, Canadians is an inevitable by-product of the collection of foreign intelligence under s 16 has been recognized since the creation of the Service. A proposal that would have required the Service to terminate an interception if a Canadian was a party to the communication was rejected as impractical by the Standing Committee on Justice and Legal Affairs in 1984 (Canada, House of Commons, Minutes of Proceedings and Evidence, Issue No 38 (June 7, 1984, at pp 65-68).

[19] At the same time, the collection, retention, and use of incidentally intercepted information raises concerns about Canadians' privacy.

[20] I received a significant amount of evidence about how the Service treats information about Canadians collected incidentally pursuant to s 16. Most of this evidence came in the form of affidavits and testimony from a senior Service employee, the Director General of the Secretariat of Deputy Director Operations (DDO), [redacted] The following description is taken largely from that person's evidence.

(2) Background

[21] In 2017, my colleague Justice Simon Noël, issued a Direction requesting the Service to provide an explanation "as to the CSIS retention practices of Canadians' communications with [foreign persons] and Condition 1 of the General Intercept and Search Warrant." The Service responded to Justice Noël's request by way of letter in which it pointed out that s 16 contemplates the incidental collection of information about Canadians as was specifically recognized by Justice Mactavish in her 2011 decision (*Re CSIS*, above). Justice Mactavish found that "properly interpreted, subsection 16(2) prohibits the interception of the communications of Canadian citizens . . . except insofar as those communications may be incidentally intercepted through the exercise of warrant powers in relation to the communications of non-Canadians" (at para 106). Accordingly, said the Service in its reply to Justice Noël, "warrants provide authority to the Service to intercept incidentally the communications and the oral communications of any person solely in the course of exercising the interception powers authorized in the warrants."

[22] The Service also explained to Justice Noël that the processing of incidentally collected information was conducted promptly and that information that did not fall within the exceptions contained in Condition 1 of the warrants was destroyed [redacted] Condition 1 states that information about Canadians shall be destroyed unless it (a) relates to activities constituting a threat to national security; (b) could be used to prevent, investigate, or prosecute a crime; or (c) relates to the capabilities, intentions or activities of any foreign state, person, or corporation for which Ministerial assistance has been requested.

[23] According to the Service, information that falls within one of the exceptions in Condition 1 would be retained in accordance with the CSIS Retention Schedule for [redacted] (although this has since been reduced in practical terms to [redacted] The information could be used in a report, however, and reports can be retained for 20 to 50 years.

[24] On receiving the Service's response, Justice Noël issued a further Direction in which he noted that the letter "raises questions as to the legitimacy of collection and retention when related to information on Canadians and even more so when such Canadians are democratically elected representatives." He directed that "this legal issue should be raised as part of a new section 16 warrant application so that the Court can have all the necessary factual and legal information to make a proper determination if required."

[25] In due course, the Service complied with Justice Noël's Direction in the application before me. As explained above, the Service also took the opportunity to raise a number of other legal issues arising under s 16.

(3) The Service's practices relating to information about Canadians

[26] The Service emphasized the scope of the current safeguards in respect of the collection of foreign intelligence pursuant to s 16.

[27] The powers available under s 16 can be invoked only if the Minister of Foreign Affairs or the Minister of National Defence personally requests, in a written Letter of Request, the assistance of the Service. Assistance will be provided only if the Minister of Public Safety and Emergency Preparedness personally responds with a written Letter of Consent.

[28] Attached to the Minister's Letter of Request is an Annex called "Rationale" setting out the specific intelligence requirements being sought. The Rationale includes "Clear Requirements/Tasking" providing particulars about the matters of greatest interest to the requesting Minister.

[29] Receipt of a Letter of Request does not automatically lead to a Service application for a warrant. Rather, the Service may begin to deploy minimally intrusive measures to gather intelligence – physical surveillance, human source contacts, and so on. If more intrusive tools are needed, the Service may then seek a warrant.

[30] According to the *DDO Directive on Section 16 of the CSIS Act* (2014), when the Service receives a request for assistance, it initially examines the request to ensure that it falls within the ambit of s 16, that it does not target Canadians, and that it does not seek information that would

normally be obtained under the Service's s 12 mandate (*i.e.* relating to threats to the security of Canada).

[31] Any information collected pursuant to s 16 is reviewed by a Communications Analyst (CA) who determines whether it has value. If not, the information is destroyed. If so, the CA will draft an internal report which is then reviewed by the CA's supervisor who verifies the relevance of the information, and ensures compliance with the Service's policies. If the report is approved, it is added to the Service's s 16 database.

[32] Internal reports prepared by a CA may form the basis of an external report drafted by a Requirements Officer (RO) whose task is to respond to the Minister's requirements as set out in the Rationale accompanying the Letter of Request. External reports have limited distribution on a need-to-know basis. Recipients must obtain permission from the Service to make further use of them. The level at which approval must be obtained varies according to the sensitivity of the contents of the report.

[33] Information that is collected incidentally about Canadians is protected in a number of ways. To begin with, access to the s 16 database is limited; it is granted only on a file-by-file basis, meaning that persons involved in analyzing foreign intelligence about one country will not have access to information about another. Access is controlled by a senior Service employee, [redacted]

[34] The Service has also adopted a policy on the minimization of information about Canadians. The *DDO Directive on Section 16 of the CSIS Act*, cited above, defines minimization as the measures taken to reduce the extent of electronic surveillance while allowing legitimate investigations to be carried out. However, a better definition of minimization for present purposes is contained in OPS-221 s 1.19:

> A term used to identify the practise whereby, unless subject to a specific exemption, any recognizable reference to a Canadian citizen, a permanent resident within the meaning of the *Immigration and Refugee Protection Act (IRPA)* or a corporation incorporated by or under an Act of Parliament or of the legislature of a province or territory, is replaced by a generic term.

[35] In other words, minimization serves to limit disclosure of the identities of Canadians (citizens, permanent residents, and companies) in all s 16 related intelligence by deleting them or replacing them with non-specific labels, such as "a Canadian company" or "a named Canadian person."

[36] There are four exemptions in OPS-221. Minimization will not occur if the reference to a Canadian:

i. Is necessary to the understanding or exploitation of the foreign intelligence;

ii. Concerns activities that could constitute a "threat to the security of Canada" as defined in s 2 of the *CSIS Act*;

iii. Concerns the prevention, investigation, or prosecution of an alleged indictable offence; or

iv. Is already in the public domain.

[37] In practice, there is more minimization in external reports than in internal reports. Generally speaking, recipients of external reports do not need to know Canadians' identities in order to understand or use the intelligence the Service provides in response to a Ministerial request. The main purpose of an external report is to respond to the Rationale contained in the Minister's Letter of Request; personal information is less likely to be relevant to that purpose. On the other hand, the raw information contained in internal reports will be difficult to understand if the identities of the persons involved are not disclosed. The Service witness provided examples of internal reports in which the identity of a Canadian was integral to the intelligence that had been gathered; without it, the information would have been virtually useless.

[38] When deciding whether to provide a Canadian's identity in an external report on the grounds that it is necessary to an understanding of the foreign intelligence, ROs do not apply any formal criteria, although the Intelligence Assessment Branch of the Service is developing guidelines. However, ROs do consider the client department receiving the report and the use to which the report will likely be put, and will sometimes limit the distribution of reports containing identifying information, or include a special caveat within the report. The RO's decision not to minimize an identity is reviewed by his or her supervisor.

[39] OPS-221 contains special guidance in respect of Canadian "public officials" and "senior public officials." The former category includes provincial and territorial legislators, mayors, deputy mayors, and municipal council members. The latter consists of a broad range of officials:

> Prime Minister, Governor General, Lieutenant Governors, Clerk of the Privy Council, Order-in-Council appointments, Provincial/Territorial Premiers, Provincial/Territorial leaders of opposition parties, Members of Parliament, Senators, Parliamentary/legislative Secretaries, Deputy Ministers, Associate Deputy Ministers, Assistant Deputy Ministers, heads of public agencies or corporations, members of the Judiciary, and Chiefs of Staff for senior public officials.

[40] The policy requires the approval of the Director of the Service or a designate before any external reports can include information or intelligence relating to public officials or senior public officials (OPS-221, s 3.1).

[41] Where information about a Canadian has been minimized in an external report, the recipient of the report can request the Service to reveal the identity of the person or company referred to; that is, it can request un-minimization. If the Service agrees to provide that information, it will be contained in a separate report so that the original report containing minimization is not altered; in other words, other recipients of the report will not receive the Canadian's identity.

[42] No particular rationale needs to be given for the un-minimization of information in an external report, and the Service does not apply any specific criteria for granting such a request. However, the standard practice is that the requester must give some reason why a person's

identity should be disclosed and provide information about the extent to which that identity will be distributed further. The request is then forwarded to the relevant operational branch for consideration. The branch considers the rationale and the source of the request. It may ask for further information before responding. The branch will also consider whether the minimized identity relates to a source, or could otherwise lead to the identification of a source; if so, the request will be denied. Similarly, if the disclosure would jeopardize an ongoing Service operation, the request will be denied.

[43] The Service's operations relating to s 16 intelligence gathering has been reviewed by the Security Intelligence Review Committee and discussed in various Annual Reports. In the early 1990s, SIRC began examining foreign intelligence retained by the Service (little use had been made of s 16 up to then). It found that the Service was not targeting Canadians or retaining excessive or unnecessary information from s 16 operations (1993-94 at p 36).

[44] By the mid-1990s, SIRC was satisfied that the Service was dealing appropriately with information about Canadians, including Canadian political figures, and was reviewing the Service's warrant applications at least annually. The number of s 16 applications was, however, growing.

[45] In the late 1990s, however, SIRC found that there were a number of instances in which the Minister's s 16 requests did not comply with the prohibition on targeting Canadians (1997-1998, at p 53).

[46] In 1999, noting that some s 16 warrants did not contain caveats about the incidental interception of communications by Canadians, SIRC recommended that Ministers seeking the Service's assistance should indicate when there is a real likelihood of those interceptions occurring, and that s 16 warrants should explicitly prohibit targeting Canadians (1999-2000 at p 30). SIRC also expressed concern about the duration of the Service's retention of information about Canadians, and suggested that reports to requesting agencies should contain only the information that was absolutely essential for the exploitation of the foreign intelligence.

[47] In the within warrant application, the Service proposes to reinforce its recognition of the limited scope of s 16 in respect of Canadians by adding the following recital indicating that the authorizing judge is satisfied that the s 16 warrant requested is not directed at any Canadians:

> I am satisfied that the warrants do not contravene the limitation stipulated at paragraph 16(2) of the *Act*. In particular, I am satisfied that the warrant powers set out herein will not be directed at any person who is a Canadian citizen, a permanent resident within the meaning of the *Immigration and Refugee Protection Act*, or a corporation incorporated by or under an Act of Parliament or of the legislature of a province.

[48] This recital has been included in s 16 warrants over the past year. It is an important addition to these warrants and, in my view, should continue to be employed. This is particularly so given the concerns expressed by SIRC over the years.

(4) Communications and privileges of elected officials

[49] A particular concern relates to the incidental interception of communications between members of federal or provincial legislatures and foreign persons or entities. Again, this is an inevitable consequence of foreign intelligence gathering. For example, a [foreign person], whose communications are intercepted pursuant to a warrant issued by the Court to the Service, may telephone a member of Parliament to discuss a matter of mutual interest or concern. The member's comments will be intercepted incidentally as a result of the warrant.

[50] The *amici* suggest that these kinds of interceptions do not impinge directly on Parliamentary privilege; however, they maintain that the values that underscore and permeate the concept of Parliamentary privilege are put in play. This requires, they say, special care and treatment of the incidentally intercepted communications.

[51] In my view, parliamentary privilege does not justify the creation of special rules or guidelines to address situations where the communications of elected officials are intercepted pursuant to s 16 warrants. First, properly understood, parliamentary privilege is not engaged by these kinds of interceptions. Second, the Service's current procedures relating to the treatment of incidentally intercepted communications of all Canadians, described above, including public officials and senior public officials, under s 16 warrants are generally adequate and consonant with the Service's s 16 mandate. However, as discussed below, I agree with the *amici* that the Service should develop criteria and guidelines on the unminimization of identifying information about Canadians.

[52] According to the *House of Commons Procedure and Practice, Second Edition, 2009*, Parliamentary privilege refers to those rights possessed by members of a legislature that are essential to their role:

> Parliamentary privilege is the sum of the peculiar rights enjoyed by each House collectively…. and by Members of each House individually, without which they could not discharge their functions, and which exceed those possessed by other bodies or individuals. Thus privilege, though part of the law of the land, is to a certain extent an exemption from the general law.

[53] As an example, to enhance their freedom to debate issues of public policy, legislators are immune from liability for defamation in respect of comments made within the Parliamentary precinct on subjects relating to Parliamentary business. That privilege is limited, and does not extend even to communications between legislators and constituents (*Pankiw v Canada (Human Rights Commission)*, 2006 FC 1544).

[54] The question whether the electronic interception of legislators' communications intrudes on Parliamentary privilege has been considered by legislative bodies, but not definitively answered, over the years.

[55] In the late 1970s, the then Speaker of the House of Commons, Mr. James Jerome, ruled that the interception of communications of a Member of Parliament raised a *prima facie* question of privilege, even when it took place outside the Parliamentary precinct, if it amounted to harassment, obstruction, molestation, or intimidation. However, a motion to refer the question to the Standing Committee on Privileges and Elections was defeated in the House, so no formal

ruling on the matter was made. (See Special Committee of the Senate on the Canadian Security Intelligence Service, *Proceedings of the Senate on the Canadian Security Intelligence Service on the subject matter of Bill C-157*; *House of Commons Procedure and Practice, Second Edition, 2009*, p 9).

[56] In 1980, a Special Committee of the British Columbia legislature concluded that the interception of a member's communications by the RCMP amounted to a breach of privilege and contempt of the legislature. Fear of intercepts, the Committee found, interfered with members' ability to perform their legislative duties, including in their homes. It stated:

> [P]arliamentary democracies flourish only when member and constituent can communicate freely, openly and candidly without having the spectre of interception . . . interfering with such communication. (at para x)

[57] Also in 1980, a Special Committee of the Yukon Assembly considered whether the wiretapping of the Minister of Justice's telephone interfered with Parliamentary privilege. Like the BC Committee, the Yukon Special Committee concluded that the actions of the RCMP amounted to a breach of privilege and contempt of the House (see Donald E Taylor, "Electronic Surveillance and Members' Privileges" (1989), 12 *Canadian Parliamentary Review* 12; David Cheifetz, "Protection of Confidential Communications of Members of Parliament" (1981), 4 *Canadian Parliamentary Review* 17).

[58] These events in BC and Yukon led the Solicitor General of Canada in 1983 to issue a *Ministerial Directive on Legislators' Privileges and Immunities in relation to Part IV.1 of the*

Criminal Code within the Precincts of Parliament, Provincial and Territorial Assemblies. The Directive required the RCMP to seek advance legal advice from the federal or provincial Department of Justice and to inform the agent designated to apply for the warrant that a privilege may be in play. In turn, the agent would have to inform the judge hearing the warrant application of the particular circumstances. Further, the responsible cabinet member – the Solicitor General at the federal level and the Attorney General in the province – was to be informed before the warrant was executed. In addition, if execution of the warrant was to take place within the precincts of Parliament or a legislature, consent of the Speaker would be required.

[59] These examples show special concern about the interception of legislators' communications. None of them, however, involved rulings by the courts on the scope of parliamentary privilege in general, or the impact that intercepting legislators' communications would have on any privilege.

[60] In the United Kingdom, the Investigatory Powers Tribunal considered the issue in 2015: *Caroline Lucas MP and Ors v Security Service and Ors*, [2015] UKIPTrib 14_79-CH.
The Tribunal noted that the general policy, referred to as the "Wilson doctrine," prohibits interception of parliamentarians' communications. However, according to the Official Guidance given to security services, the Wilson doctrine applies only where the communications of members of parliament are deliberately, not incidentally, targeted. Even so, if special measures are followed, the communications of a Member of Parliament can be targeted and intercepted under warrant. Those measures include special authorization by designated officials, and the

involvement of the Secretary of State, the Cabinet Secretary, the Prime Minister, and a special legal advisor charged with retaining and handling the intercepted communications.

[61] Accordingly, notwithstanding the Wilson doctrine, there is no absolute prohibition against the targeted interception of parliamentarians' communications in the United Kingdom, but great care is taken to ensure that interceptions are justified and that their fruits are carefully handled. Note, however, that these UK warrants are not subject to judicial authorization.

[62] The Supreme Court of Canada has pronounced on the scope of Parliamentary privilege generally but not on the question of intercepting parliamentarians' communications (*Canada (House of Commons) v Vaid*, 2005 SCC 30). At issue in *Vaid* was Parliament's jurisdiction to deal with rights owed to employees of the House of Commons as compared to the jurisdiction of other bodies, such as the Canadian Human Rights Tribunal, with responsibilities for federal public servants generally.

[63] *Vaid* makes clear that defining the scope of Parliamentary privilege falls to the courts, not to the legislatures. The first step is to determine whether "the existence and scope of the claimed privilege have been authoritatively established" in respect of the Canadian Parliament or the UK House of Commons (at para 39). Where there has been no authoritative ruling on the question, the court must "test the claim against the doctrine of necessity, which is the foundation of all parliamentary privilege" (at para 40). While not bound by them, courts will give "considerable deference" to the views of legislators on the scope of autonomy they consider necessary to their function (at para 40).

[64] It is the courts, then, that define the scope of a privilege, while legislators determine the merits or the appropriateness of its exercise.

[65] To determine what is "necessary," one must consider what is needed "to protect legislators in the discharge of their legislative and deliberative functions, and the legislative assembly's work in holding the government to account for the conduct of the country's business" (at para 41). The requirement of necessity imports "important limits" on the scope of the privilege (at para 43). For example, there may be words or actions that are unrelated to parliamentary business and would, therefore, fall outside the parameters of the privilege. Courts will recognize as privileged only those activities that are "so closely and directly connected" with parliamentary functions that "outside interference would undermine the level of autonomy required to enable the assembly and its members to do their work with dignity and efficiency" (at para 46).

[66] In *Vaid*, the Court found that parliamentary privilege did not oust the jurisdiction of the Tribunal, and laid out a number of general principles, the most pertinent of which for present purposes are:

- Parliamentary privilege includes the immunity necessary for members to do their legislative work.

- The test for necessity is what the dignity and efficiency of the House require. The concept of dignity and efficiency is linked to the autonomy that is necessary to enable Parliament and its members to do their jobs.

- The party seeking to rely on the immunity provided by parliamentary privilege has the onus of establishing it.

- Once a category or sphere of activity has been established, it is for Parliament to decide whether the exercise of the privilege is necessary or appropriate.

- Existing categories include: freedom of speech, control by the House over debates and proceedings in Parliament, the power to exclude strangers from proceedings, disciplinary authority over members and non-members who interfere with the discharge of Parliamentary duty, and immunity of members from subpoenas during a parliamentary session.

- The mere affirmation by a legislative body that a certain act is a breach of its privileges will not oust the courts from enquiring and deciding whether the privilege claimed really exists.

- The courts will look more closely at cases in which the privilege claimed will have an impact on persons outside the legislative assembly, than those in which the matters are entirely internal to the legislature.

[67] The Court did not refer to the kind of the privilege discussed above that was recognized in respect of the BC and Yukon legislatures; nor did it address the issue of immunity from wiretapping within the categories of privilege currently recognized. But it is clear from its reasoning that it would fall to the courts, not the legislators, to determine whether any such

privilege existed. Accordingly, while the views of the BC and Yukon legislators merit considerable deference, they are not determinative.

[68] In sum, there is no clear legal authority for the proposition that intercepting the communications of parliamentarians, in itself, violates Parliamentary privilege. Only if the interception interfered with a member's ability to conduct parliamentary business or otherwise constituted harassment or intimidation, would the question of privilege arise.

[69] For s 16 purposes, a parliamentarian, being Canadian, could not be directly targeted. However, as mentioned, his or her communications could be intercepted incidentally pursuant to a valid s 16 foreign intelligence warrant. Not being a target, it is difficult to see how an interception could amount to an attempt to interfere with the member's ability to conduct parliamentary business. Similarly, if the member is not the target, it is unlikely that the execution of the warrant would take place within the Parliamentary precinct. There would be no need to obtain the permission of the Speaker of the House to conduct an interception.

[70] In any case, however, as explained above, the *amici* do not assert that parliamentarians enjoy actual immunity from incidental interceptions of their communications in the foreign intelligence gathering context. Therefore, I need not rule definitively on that question. I do, however, have to consider whether applications for, and the fruits of, those interceptions require special treatment.

[71] The *amici* suggest that the current policies that apply to the incidental interception of parliamentarians' communications provide inadequate protection of Canadians' privacy. They propose that the Court impose conditions on the Service relating to the retention, disclosure, and minimization of information about elected officials pursuant to the authority to include terms and conditions on the execution of warrants issued by the Court (*CSIS Act*, s 21(4)(*f*)). They also suggest that the Court play a supervisory role. In particular, they submit that the Service should be required to return to the Court for permission to retain incidentally collected communications of Canadians, to distribute information collected, or to unminimize the identities of Canadians. They note that, in the case of incidental collection of communications of elected officials, these requirements would permit the Court to rule on any issues of parliamentary privilege that might arise. While they do not see the need for special rules for parliamentarians, they note that clearer rules about Canadians generally would also foster communications between elected officials and their constituents.

[72] I largely agree with the *amici*. Greater protection should be granted to information about Canadians incidentally collected in the gathering of foreign intelligence. As mentioned, there are no formal criteria guiding Service employees or others on unminimizing identities of Canadians. Without guidelines, decisions about the retention, disclosure, and distribution of this information is left to individual discretion. More is required, especially since this is information that is acquired merely as a by-product of the Service's mandate to collect foreign intelligence. I would not go so far, however, as to impose a blanket obligation on the Service to return to the Court for permission to retain incidentally collected information about Canadians.

[73] The information about Canadians that the Service obtains in this fashion merits special care and respect. That is even more true for information about public officials and senior public officials, as the Service's policies already recognize. As explained, it is not parliamentary privilege itself that animates the need for extra care; indeed, few officials could mount any real claim to privilege. The concern about gathering information about public officials is that the Service may be intercepting highly sensitive communications emanating from persons charged with the governance of Canada. That information, particularly information about the identity of the Canadian persons involved, must be carefully handled.

[74] In my view, the Service must develop guidelines for distributing and unminimizing the identities of Canadians whose communications have been incidentally intercepted. It should advise the Court of the content of those guidelines and permit the Court an opportunity to comment on them. In individual warrant applications, the Service should continue to inform the Court when there may be incidental interceptions of Canadians' communications. It should also specifically disclose when there is a possibility that the communications of an elected official or other public servant may be intercepted. This disclosure requirement will permit the Court, where appropriate, to attach terms and conditions on the execution of the warrants it issues. Those terms and conditions could include imposing a requirement on the Service to return to the Court for directions on the handling of information collected, as proposed by the *amici*.

C. *The Relationship Between s 16 and s 12*

[75] An ongoing concern of members of the Court is the potential overlap between, or the blending of, the Service's mandates under s 16 and s 12. Accordingly, I asked the Service to address this issue based on the observation that some recent requests for warrants under s 16 for foreign intelligence purposes resemble applications under s 12 for warrants to investigate threats to national security. The resemblance arises from two features of these s 16 applications. First, they have related, in essence, to matters that could easily be described as threats to the security of Canada. Second, they sometimes involve targets who are already the subject of warrants under s 12.

[76] The concern that arises from this situation is that s 16 could come to be used as an alternative or a supplement to s 12, contrary to the intention of Parliament when enacting the *CSIS Act*. When requesting a warrant, the Service may sometimes perceive an advantage in proceeding under s 16 rather than s 12. Section 16 arguably has a broader scope relating as it does to the collection of information about "the capabilities, intentions or activities" of any foreign state or non-Canadian person. By contrast, s 12 applies only to the collection, analysis, and retention of information relating to "threats to the security of Canada," a term that is statutorily defined.

[77] A potential scenario would be this: If the Service believed that a foreign person in Canada was involved in some activity that posed a danger that did not necessarily fall within the definition of a "threat to the security of Canada," it could seek a warrant under s 16 to determine the person's intentions, capabilities, or activities. Of course, there are constraints that apply to s 16. The Service could seek a foreign intelligence warrant only if its assistance was requested by

the Minister of National Defence or the Minister of Foreign Affairs, and with the consent of the Minister of Public Safety and Emergency Preparedness. Further, the Service could collect information only within Canada. The Service could not directly target a Canadian person. However, if a Canadian was known to be in contact with [redacted] or other foreign persons, the Service could target the latter and "incidentally" intercept the communications of the former. In effect, a Canadian could become the indirect target of a foreign intelligence warrant, even though s 16 specifically prohibits the targeting of Canadians.

[78] I hasten to point out that there is no suggestion that the Service has ever used s 16 in this manner. The concern arises from the potential to use s 16 in this way and, as mentioned, the facial similarity between some recent s 16 applications and s 12 requests.

[79] The Service addressed this issue by presenting the evidence of two senior and experienced Service members. This evidence satisfies me that the Service has taken steps to ensure that there is no operational interaction between the Service's foreign intelligence activities under s 16 and its s 12 mandate relating to security intelligence. The following is a summary of that evidence.

[80] The Service's operations, whether under s 12 or s 16, or otherwise, are subject to internal policy directions. For matters relating to national security, if the Service has grounds to suspect that a person or group poses a threat, it may request internal authority to begin an investigation. Those charged with reviewing these requests help ensure that the proposed investigation

complies with the Service's policies and the governing law, and amounts to a proportional response to the perceived threat.

[81] Information collected under s 12 is reviewed by an analyst who determines its intelligence value. Information is retained only as permitted by the Service's retention schedule. Information with no intelligence value is destroyed after [redacted] Valuable information may be retained for 20 or 25 years after the last action on the file. Information that was collected pursuant to a warrant is subject to the conditions set out in it. For example, specific time periods for destruction of information are provided for solicitor-client communications and the communications of third parties.

[82] Policies also govern the preparation of operational reports. If the analyst concludes that the information collected is valuable, and that the applicable policies and conditions have been respected, he or she will prepare an operational report. These reports are reviewed by supervisors who verify the relevance of the information collected, ensure that the Service's policies have been respected and, if the information was gathered under a warrant, confirm compliance with the applicable terms and conditions. If the supervisor approves the report, it will be stored in the Service's s 12 database. These reports may then form the basis of other intelligence reports submitted to persons within the Government of Canada, with the caveat that they not be used or distributed further without the Service's permission.

[83] Information collected under s 16 is treated similarly, but separately. Again, an investigation must first be authorized. Here, though, that authority comes from the Minister of

Public Safety's consent to a written request for assistance from the Minister of Foreign Affairs or the Minister of National Defence. Once the Service receives the request and the consent, it will begin gathering relevant information and, if there are reasonable grounds to believe that the powers available under warrant are necessary, it will seek the Court's authority under s 21 of the *CSIS Act*.

[84] The Service itself recognizes the possibility of a co-mingling of s 12 and s 16 mandates. The Service's operations policy acknowledges that parallel investigations may be necessary in some circumstances; however, it specifically provides that "operations conducted to support an investigation under one section of the CSIS Act will not be used as a pretext for conducting operations pursuant to another section of the *Act*." (Emphasis in the original.)

[85] Over the years, the Security Intelligence Review Committee has repeated similar concerns.

[86] In 2006-2007, SIRC reported that the Inspector General had noted considerable overlap between s 12 and s 16 operations. For example, agents tasked with obtaining information abroad under s 12 provided intelligence relevant to s 16. Indeed the Inspector General wondered whether the geographical constriction of s 16 ("within Canada") was a meaningful limitation on the Service's powers (p 37).

[87] Further, in 2009-2010, SIRC noted that the Service had referred to simultaneous s 16 and s 12 investigations as "blended collections", where the Service was engaged in s 12 and s 16

operations against the same targets. It observed that if this situation were to continue, the Service could become a body with equivalent foreign intelligence and security intelligence mandates, which was not the original intention of Parliament. It recommended that the Government of Canada provide direction or guidance to the Service on its expanded role in collecting foreign intelligence (2009-10 at p 15).

[88] In 2013, SIRC again detected a potential tension between the Service's two mandates under ss 12 and 16. The Service itself felt its s 16 non-threat-related mandate had the potential to distract it from its primary role of gathering threat-related intelligence under s 12 (2012-13 at p 16).

[89] In 2015, SIRC commended the Service for adapting its s 16 procedures to coordinate and streamline its priorities and activities. The Service had also made changes to distinguish between its s 12 and s 16 operations (2014-15 at p 22).

[90] The *amici* emphasize that the Service must not make any "colourable use" of a s 16 foreign intelligence warrant to collect s 12 security intelligence. This means that the Service should seek a separate s 12 warrant if its s 16 investigation discloses a threat to national security. In addition, where parallel investigations are ongoing, the Service must satisfy the discrete requirements for s 12 and s 16 warrants separately and independently, and inform the judge receiving each warrant application of the existence of the other.

[91] The *amici* accept, based on the evidence filed on this application, that the Service is currently abiding by the procedures they propose. They note, however, that the heightened protection in respect of incidentally collected information about Canadians that they recommend (as discussed above) would help ensure that the Service does not use foreign intelligence warrants to collect security intelligence about Canadians.

[92] In my view, the Service is acutely aware of the Court's (and SIRC's) concerns in this area. It has addressed those concerns in a serious way in both its operations and policies. I see no need to propose any further ~~any~~ action on the Service's part. I have no doubt, however, that members of the Court will continue to expect the Service to address any concerns the Court may have about future "blended collections." In addition, I agree with the *amici* that stronger protection in respect of incidentally collected information about Canadians would help dispel some of those concerns.

D. *Proposed Changes to the s 16 Warrant Templates*

[93] The AGC proposes a number of changes to the templates that provide a presumptive format and content for the various kinds of foreign intelligence warrants the Court issues pursuant to s 16. These changes fall within three categories:

i. Incidental changes bringing the s 16 warrant templates into line with s 12 warrants.

ii. Amendments clarifying the scope of particular powers.

iii. New powers.

[94] In this section, I will deal only with proposed changes that do not amount to any significant expansion of the powers exercised under s 16 warrants. I will deal elsewhere with the comparatively substantial changes the Service seeks, such as those relating to the use of CSS and [redacted] surveys.

(1) Incidental changes to warrant templates

[95] The Service proposes a number of amendments that would bring s 16 warrant templates in line with s 12 templates. These include:

- Inclusion of a new condition clarifying the meaning of the word "destroyed" when creating an obligation on the Service to destroy information. "Destroyed" would be defined as meaning that the information "shall not be retrieved by the Service or by any other agency or person on its behalf."

- Amendment of the definition of "residence" to include any place in which a Regional Director General has reasonable grounds to believe a person resides.

- Inclusion of a definition of "test data" and a corresponding condition allowing the Service to retain intercepted communications solely for purposes of developing or maintaining its interception and collection capabilities.

- Replacing the definition of [redacted] with [redacted] to provide a more accurate description of the means used to locate a person or vehicle [redacted]

- Expanding the description of places where warrants can be executed to include [redacted]

- Adding a power to intercept [redacted]

- Adding a power to obtain images of persons named in the warrant or attending places specified in the warrant.

- Amending the retention condition of the warrants by including an assessment period of [redacted] after which the collected information (other than information from [redacted] must be destroyed unless the stipulated conditions have been met (ie the information relates to a threat, a crime, or the capabilities, intentions, or activities of the foreign state).

- Inclusion of a new condition allowing the Service to create backups of collected intercepted information.

- In the [redacted] Warrant, adding a power to obtain information about [redacted]

[96] The *amici* raised no significant concerns about these changes. I agree that the proposed modifications are routine and raise no legal issues.

(2) Clarifying the scope of some powers

[97] The Service wishes to clarify that it has the lawful authority to [redacted] This would enable the Service to intercept [redacted] without having to [redacted]

[98] Neither of these two activities would require any amendment to the warrants or involve the use of any new powers.

[99] The Service also seeks to clarify its power to search [redacted] This is not, strictly speaking, a new power but the Service proposes that the locations where searches can be carried out be expanded to include, [redacted]

[100] Again, the *amici* raised no concerns in this area, and I see no legal issues arising from the proposed amendments.

(3) New powers or locations

[101] The Service seeks two powers that it has not previously sought for purposes of s 16 investigations – search of [redacted] and the search of [redacted] In both cases, the searches would be confined to [locations used by foreign persons]

[102] These kinds of powers are frequently used in the s 12 context, and there is no obvious reason not to permit them for s 16 investigations.

(4) Conclusion on warrant templates

[103] Many of the amendments described above have been the subject of submissions and discussions with the Court following ~~on~~ the *en banc* hearing giving rise to Justice Simon Noël's decision in the *Associated Data* case (*Re X*, 2016 FC 1105). These discussions are ongoing. Any changes or improvements to the wording of the s 12 warrant templates should generally result in corresponding changes to the warrant templates applicable in the foreign intelligence context.

III. Issue Two – Does s 16 authorize use of CSS technology?

[104] The Service seeks to confirm that its authority pursuant to s. 16 of the *CSIS Act* includes the ability to capture information through use of cellular site simulators (CSS). CSS can be used to obtain data emitted by mobile devices, namely IMSI (International Mobile Security Identity) and IMEI (International Mobile Equipment Identity). The former reveals the country where the user's cellular account is located, the network code for the service provider, and a subscriber identity number assigned by the service provider. The latter indicates the make, model, and serial number of the device. No other attributes of targeted devices are captured through use of CSS. Nor is any content of communications captured. The sole purpose of CSS is to obtain information that could later be used in an application to the Court for a warrant to intercept the user's communications.

[105] This Court, in a decision authored by Chief Justice Paul Crampton, has addressed the use of CSS in the context of s 12 of the Act, that is, for purposes of investigating threats to national security (*Re X (CSS)*, 2017 FC 1047). The Chief Justice concluded that the use of CSS amounted to a search because users of mobile devices had a reasonable expectation of privacy in respect of the information CSS technology could capture. However, he found that use of CSS without a warrant was lawful so long as the Service took measures to minimize the intrusion on privacy by refraining from intercepting communications or information stored on the device, destroying any information collected incidentally from third parties, and desisting from using the information for purposes of geo-location. While the information available through CSS could assist the Service to create a thin personal profile of the user, thereby engaging s 8 of the Charter, the Chief Justice found that the warrantless searches were not unreasonable given that they were narrowly targeted, highly accurate, and minimally intrusive.

[106] The question before me is whether the analysis carried out by the Chief Justice in the national security context applies equally or, at least, comparably in the context of foreign intelligence gathering. At several points, the Chief Justice emphasized the special nature and purpose of s 12 of the Act, in particular, the state interest in obtaining information that would further its duty to protect national security. As discussed, the nature and purpose of s 16 differs from that of s 12. Does that difference affect the lawfulness of the Service's use of CSS technology without a warrant? To answer that question, I will review those parts of the Chief Justice's decision where the differences between the nature and purposes of s 16 and s 12 may influence the analysis. I will then consider other differences between the two provisions.

[107] The Chief Justice began by making clear that warrantless searches are presumptively unreasonable and contrary to the protection in s 8 of the Charter against unreasonable searches and seizures. Nevertheless, a search could be found to be reasonable if it was authorized by law, the law was reasonable, and the search was executed reasonably. He found that, under s 12, the Service had an obligation to collect, analyze, and retain information and intelligence about activities posing a threat to national security (para 196). The Act also sets out the circumstances when the Service should obtain a warrant (s 21). However, the Act does not require the Service to obtain a warrant whenever it seeks to gather information relating to national security even when a person's reasonable expectation of privacy is at stake. He found that there is a range of minimally intrusive activities the Service can carry out within its national security mandate without having to obtain a warrant (para 198), again, so long as the law authorizes those activities, the law is reasonable, and the means of carrying out the search are reasonable.

[108] By contrast, under s 16, the Service may (not shall) assist the respective Ministers in collecting foreign intelligence; its mandate is neither as strong nor as direct as its national security role. As is the case with s 12, though, the Service can pursue its s 16 mandate by applying for a warrant under s 21. Still, while the differences between the two statutory mandates are clear, there is no basis for finding that the requirements for a warrant differ on that ground alone. Just as the Service can collect some forms of information relating to national security under s 12 without having to obtain a warrant, so, too, can it assist in gathering some forms of foreign intelligence without a warrant. The Act provides the Service the authority to collect both kinds of information and intelligence. The requirement for a warrant is not engaged for all intrusions into reasonable expectations of privacy, only in respect of searches that would

otherwise be unreasonable, as the Chief Justice found in respect of s 12 (para 199). I find that minimally intrusive searches are authorized by s 16 without the requirement of a warrant.

[109] The Chief Justice found that s 12 was a reasonable law, considering its nature and purpose, the degree of intrusiveness it authorizes, the mechanism of intrusion, the availability of judicial supervision, and other checks and balances. The first of these criteria, the nature and purpose of the applicable statutory provision, differs significantly as between ss 12 and 16, as discussed above.

[110] The Chief Justice considered the nature and purpose of s 12 to be the assignment of responsibility to the Service, where strictly necessary, to collect, analyze, and retain information and intelligence in respect of activities it reasonably suspects constitute a "threat to national security", a statutorily defined term (s 2). He described this role as "critical, central and arguably essential". He rejected arguments of the *amici* before him that the reasonable suspicion standard was unconstitutionally low, noting that that standard had been approved by the Supreme Court of Canada in cases where privacy interests were limited, important public interests were at stake, or the search method involved was highly accurate (paras 206-207). Each of those circumstances, he concluded, was present in respect of searches using CSS for s 12 purposes – minimal intrusion, pressing national security concerns, and high precision.

[111] There are at least three notable differences in the nature and purpose of s 16 as compared to s 12. First, the role given to the Service under s 16 is permissive, not mandatory; the Service "may" assist the named Ministers in the collection of information and intelligence relating to

foreign persons or states. Realistically, however, given that the provision requires a personal request in writing of the Minister of National Defence or the Minister of Foreign Affairs, and the personal consent in writing of the Minister of Public Safety and Emergency Preparedness, it is difficult to conceive of a situation where the Service would decline to provide assistance on request.

[112] Second, the Service's s 16 mandate is not a direct responsibility to collect intelligence. The Service's role is to assist the named Ministers; its role cannot be described as "critical, central and arguably essential". As Justice Noel has noted, s 16 has an "assistance or policy oriented goal, rather than a threat related one" (*Re X*, 2018 FC 738 at para 54). However, it is, no doubt, an important mandate and one which the Ministers likely consider to be highly valuable to the discharge of their functions. But it is not on the same scale as the Service's s 12 core mandate to investigate threats to national security. As discussed, the Service's foreign intelligence role has always been seen as, at most, secondary to its national security mandate.

[113] Third, s 16 does not require that the collection of the information or intelligence be "strictly necessary" or set out a standard comparable to the "reasonable suspicion" threshold. Nor is there any statutory definition of the "capabilities, intentions or activities" of foreign entities that would limit the scope of the Service's inquiries. The Service's s 16 role is inherently broader than its s 12 mandate.

[114] Again, while the mandate given to the Service under s 16 differs in important ways from its s 12 role, that is not the equivalent of stating that the nature and purpose of s 16 is somehow

less important or less vital to Canada's interests than those animating s 12. In s 16, Parliament envisioned the Service playing a significant role, albeit secondary to its s 12 mandate, in furthering Canada's interests in national defence and international affairs. Canada's capacities to defend itself and to conduct productive relations with other states are arguably as essential to its sovereignty as its ability to combat threats to its security.

[115] The *amici* argue that this last factor, particularly the absence of a reasonable suspicion standard, sets s 16 apart from s 12 in this context. In their view, to pass constitutional muster, a reasonable suspicion standard would have to be read into s 16; that is, the Service would be entitled to use CSS technology pursuant to s 16 only where it had reasonable grounds to suspect that a foreign person possessed information relating to the capabilities, intentions, or activities of a foreign state that would assist the Minister in the conduct of Canada's international affairs or national defence.

[116] I disagree. The absence of a reasonable suspicion threshold is not constitutionally fatal. Section 16 contains other requirements that, in this context, provide an adequate substitute for the reasonable suspicion standard. The Service can gather foreign intelligence only if the Minister of Foreign Affairs or the Minister of National Defence makes a personal written request for assistance and the Minister of Public Safety and Emergency Preparedness responds with a personal written consent. The Service acts only after two senior Ministers of the Crown have concluded that the collection of foreign intelligence is required to protect Canada's interests in international affairs or defence. It falls to these Ministers to determine the appropriateness of tasking the Service to execute its foreign intelligence mandate. I have no basis for questioning

the *bona fides* of the Ministers or doubting their capacity to determine what is in the best interests of Canada. In addition, of course, if the Service later seeks to employ more intrusive powers, the Court retains a discretion in respect of the issuance of warrants under s 21.

[117] Further, in practical terms, it is unlikely that the Service, acting pursuant to its foreign intelligence mandate, would expend scarce resources in trying to collect information from persons who are unlikely to have knowledge of a foreign state's capabilities, intentions, or activities. In this way, s 16 is somewhat self-limiting, given that foreign intelligence gathering is not at the core of the Service's *raison d'être*. This distinguishes it from the Service's role under s 12, which is critical, central, and arguably essential. It is far more likely that the Service would be inclined to overreach in executing its s 12 mandate than in its s 16 role.

[118] In my view, there exist sufficient safeguards constraining the potential over-extension of the Service's foreign intelligence role to satisfy s 8 of the Charter in respect of minimally intrusive searches, such as the use of CSS, without a warrant.

[119] Therefore, in this context, I do not see a significant difference between the nature and purpose of s 16 as compared to s 12. In both areas, the Service's role furthers pressing national interests.

[120] In addition, though s 16 may lack the limiting language of s 12, it contains an essential constraint that does not apply to s 12 – s 16 targets only foreign persons and states, not Canadians. Section 16's scope is broad; its application narrow.

[121] Parliament has recognized that the Service should have greater leeway in collecting information and intelligence about foreign entities in Canada for defence and international relations purposes than in investigating threats to the security of Canada.

[122] The point to be taken from the limits in s 16 is that they constrict the Service's powers in a manner consistent with its mandate to assist in protecting Canada's national defence and furthering its international relations. There are clear limits on the Service's authority under s 16 to execute minimally intrusive powers, such as the collection of data through CSS technology.

[123] The final factor to consider in respect of s 8 of the Charter is whether the search carried out – a CSS operation – is conducted in a reasonable manner. Chief Justice Crampton concluded, in the s 12 context, that the search was, indeed, reasonable. He considered the following factors:

- IMSI and IMEI captured from third parties was deleted or destroyed before any analysis of it was done;

- CSS operations have no discernible impact on the target's use of a device; in particular, CSS activities do not cause the user to drop calls, or prevent users from placing a 911 call; and

- CSS equipment cannot intercept the content of communications or capture information stored on a device (at paras 238-242).

[124] The same factors exist for CSS operations conducted pursuant to s 16. I agree with the Chief Justice that the manner in which CSS operations are conducted is reasonable.

[125] Accordingly, I find no conflict between the warrantless use of CSS and s 8 of the Charter. Section 16 provides a sufficient and reasonable statutory basis for warrantless searches, so long as they are minimally intrusive and conducted in a reasonable manner.

IV. Issue Three – Does s 16 authorize interception of [redacted] data?

[The redactions in the following section concern technology that allows the Service to collect certain information from mobile devices. The Court concludes that the Service may use this technology, without a warrant, to obtain a specific subset of that information to identify that device for future purposes. However, the Court notes that the technology also allows the Service to acquire information from mobile devices that might permit the Service to learn about an individual's private activities and personal choices. The Court holds that the Service requires a warrant to use the technology to acquire this further information.]

[126] The Service submits that the interception of [redacted] data is essentially akin to CSS operations in that both are minimally intrusive searches conducted pursuant to valid and reasonable statutory authority (s 16) and are carried out in a reasonable manner.

[127] I disagree. Interceptions of [redacted] data capture more personal information than CSS operations. They require a warrant.

[128] I will first describe the technology relating to [redacted] interceptions and the information that can be retrieved with it. I will then consider whether s 16 provides sufficient authority for those interceptions or whether a warrant is required.

[129] The Service and the *amici* agree that [redacted] surveys do not contravene the *Radiocommunications Act* (RSC 1985, c R-2, s 9(1)(*b*)) or the *Criminal Code* (RSC 1985, c C-46, ss 184, 430(1.1)(*c*)). I concur with their submissions and need not say anything further on that point. I note that Chief Justice Crampton came to a similar conclusion in respect of CSS operations ((*Re X (CSS)*, above, at paras 82-106).

(1) The Technology

[130] The following overview is taken largely from the affidavit and testimony of [redacted] a Service employee with expertise in the area of [redacted]

[131] [redacted]

[132] [redacted]

[133] [redacted]

[134] [redacted]

[135] [redacted]

[136] The Service engages in what it calls "[redacted] surveys." In a survey, the Service obtains [redacted] in an effort to identify a particular device used by a target of an investigation.

[137] A survey involves the use of a device specially configured to capture [redacted] This kind of device can be portable or stationary. In either case, they are passive; [redacted] They do not intercept the contents of any communication or any [redacted] activity – they simply collect [redacted] An analysis of [redacted] can permit the Service to identify the particular device that a target is using.

[138] [redacted]

[139] [redacted]

[140] According to Service policy, surveys last no longer than [redacted] If the [redacted] target's device has not been identified within that period of time, all information collected in the survey will be destroyed. If the [redacted] target's device has been identified, the Service will retain it.

[141] The object of [redacted] surveys is to determine the [redacted] devices used by targets of investigation. With [redacted] the Service, armed with a warrant, can then begin to intercept the target's [redacted] As with the use of CSS, obtaining [redacted] enables the Service to seek the authority to conduct more intrusive searches armed with a warrant.

[142] The Service makes clear that the only unique, permanent, and identifiable information it obtains through [redacted] surveys are [redacted] However, that is not the only information that is gathered.

[143] The Service also obtains ancillary information [redacted] Ancillary information about devices includes [redacted] The Service retains this information if it relates to [redacted] In other words, if the Service obtains [redacted] for a target's device, [redacted] and the ancillary information associated with the device will be retained.

[144] Ancillary information [redacted] includes [redacted] The Service's own survey devices also generate ancillary information [redacted]

[redacted] Most useful to the Service are [redacted] of the survey device which establish [redacted] when the survey was conducted.

[145] The Service maintains that the two most useful pieces of information it captures through surveys are [redacted] The target's [redacted] are obtained through [redacted] It is only [redacted] that are revealed, not the [redacted] However, some information, such as the target's [redacted] can sometimes be gleaned [redacted]

[146] The [redacted] will tell the Service, for example, [redacted] This may allow the Service to determine the target's [redacted] behaviour patterns." In addition, that information may support a warrant application by the Service authorizing it to intercept the target's [redacted] through particular means.

[147] For example, if the target's [redacted] reveals that he or she usually [redacted] this may allow the Service to make use of [redacted]

[148] [redacted]

(2) Does s 16 provide sufficient legal authority?

[149] The Service submits that the most valuable information it obtains in support of its s 16 mandate often comes from the intercepted communications of those [foreign persons] [redacted] who are associated with [foreign states, groups of foreign states, or foreign corporations] in respect of which the Service is currently assisting the Minister [redacted]

[150] To obtain a warrant to carry out these interceptions, the Service must present reasonable grounds to believe that [a foreign person or persons] will be sending or receiving communications over a particular [redacted] device that is owned or leased by them [redacted] Similar to the use of CSS technology, [redacted] surveys allow the Service to obtain the unique electronic identifiers associated with the devices

which, in turn, will permit the Service to conduct warranted interceptions [redacted]

[151] The Service concedes that the use of [redacted] surveys to obtain [redacted] amounts to a search for purposes of s 8 of the Charter. However, the Service maintains that these searches constitute a minimal intrusion on individuals' expectations of privacy. [redacted], according to the Service, is similar to the IMSI and IMEI information collected through CSS and no breach of s 8 takes place when the Service obtains that kind of information without a warrant. [redacted] reveals nothing about the user.

[152] In respect of [redacted], the Service contends that the information it obtains about a user's [redacted] is "often relatively weak and non-invasive." At most, it tells the Service [redacted]

[153] Further, the Service argues that s 16 provides reasonable lawful authority for conducting [redacted] surveys that generate [redacted] Parliament, says the Service, has explicitly authorized the Service under s 16 to collect foreign intelligence, within Canada, to assist the Ministers of Foreign Affairs and Defence in determining the capabilities, intentions, or activities of foreign persons.

[154] The Service submits that s 16 complies with the requirement that the statutory basis for a warrantless search be transparent in its grant of official powers, and that it set out clear criteria (citing *R v Spencer* [2014] 2 SCR 43 and *R v Shoker* [2006] 2 SCR 44). In addition, the Service

argues that s 16 does not establish an unconstitutionally vague standard (as described in *R v Nova Scotia Pharmaceutical Society*, [1992] 2 SCR 606).

[155] In any case, says the Service, a low standard is appropriate in this context where privacy interests are reduced and state objectives predominate (*R v Chehil*, 2013 SCC 49 at para 23; *Re X (CSS)*, above, at para 206).

[156] In addition, the Service points to a number of features of s 16 that it says are indicative of its reasonableness. These factors largely track the submissions the Service put forward in respect of CSS operations, discussed above, but bear repeating in this context.

(a) *Nature and Purpose:*

[157] Section 16 fulfills an important state purpose, namely, the collection of foreign intelligence to assist the Ministers in relation to the defence of Canada and its international affairs.

(b) *Criteria and Limits:*

[158] The provision contains objective criteria and strict limits, notably, the requirements that a Minister request the Service's assistance in writing; that the Minister of Public Safety must personally consent to the assistance; that the assistance be connected to a foreign state's

capabilities, intentions, or activities; that Canadians not be targeted; and that the assistance must take place within Canada.

(c) *Balance:*

[159] Section 16 strikes a balance between the public interest in the collection of foreign intelligence and personal privacy. The Ministers must weigh these factors before initiating a request for assistance and engaging the Service's use of investigatory techniques.

(d) *Minimally Intrusive:*

[160] Since the Service can invoke the intrusive warranted powers under s 21 of the Act in pursuit of its s 16 mandate, it follows that s 16 allows for the collection of information through minimally intrusive means without a warrant.

(e) *Accuracy:*

[161] The manner in which the Service conducts [redacted] surveys ensures that the information it collects accurately identifies the device being used by the target and filters out information relating to other devices.

(f) *Accountability:*

[162] The Service is accountable for its activities to the Minister of Public Safety and is bound by the Ministerial Direction for Operations and Accountability. In addition, the conduct of the

Service was reviewed by the Security and Intelligence Review Committee (SIRC); it is now accountable to the National Security and Intelligence Agency (NSIRA).

[163] The Service also maintains that the other limits that s 12 contains – that collection is strictly necessary and that there exist reasonable grounds to suspect – are not appropriate in the s 16 context.

[164] The *amici* point out, however, that a warrantless search is presumptively unreasonable for purposes of s 8 of the Charter (*R v Collins*, [1987] 1 SCR 265). To conform with s 8, a warrantless search must be expressly authorized by a reasonable law and be carried out reasonably. The *amici* assert that the searches that result from [redacted] surveys are not authorized by s 16 and the power to conduct them cannot be implied.

[165] The *amici* also contend that these searches are more than minimally intrusive and, therefore, that they can be conducted only pursuant to a warrant. In particular, these kinds of searches permit investigators to build personal profiles of targets [redacted]

[166] I have already found that s 16 provides a sufficient, reasonable statutory basis for conducting warrantless, minimally intrusive searches, namely, capturing IMSI and IMEI

information through reasonably-conducted CSS operations. I find the same is true in respect of the use of [redacted] surveys, as described above, to capture [redacted] of targets' devices. [redacted] reveals nothing personal about the target. It simply permits the Service to identify the device for future purposes. Essentially, [redacted] are analogous to IMSI and IMEI in the CSS context.

[167] Accordingly, I agree with the Service that s 16 provides a reasonable statutory basis for capturing [redacted] of targets' devices through [redacted] surveys.

[168] I am also satisfied that minimally intrusive [redacted] surveys conducted pursuant to s 16 are carried out reasonably. As with CSS technology, there is no impact on any private communications, [redacted] or other private information stored in the device. Any third-party information collected is destroyed.

[169] However, I come to a different conclusion regarding the other information the Service would obtain through [redacted] surveys – [redacted]

[170] Again, the Service concedes that [redacted] surveys are searches but argues that, as with CSS operations, these surveys are minimally intrusive and should not require a warrant.

[171] It is important to note, however, in respect of [redacted], the kind of search that is in issue here. The target of a search would have a strong interest in keeping their personal

activities private, and have an obvious subjective expectation of privacy. That expectation would be reasonable in the circumstances.

[172] As described above, [redacted] may tell investigators about the target's private activities and allow inferences to be made about the person's personal choices. The significance of the information collected is an important factor to consider in this context (*R v Spencer*, 2014 SCC 43 at para 18, 26-31; *R v AM*, 2008 SCC 19 at para 38).

[173] In *Spencer*, Justice Thomas Cromwell, for the Court, underscored the need for a purposive approach to s 8 issues, one that seeks "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" (para 15). In particular, in determining whether a person had a reasonable expectation of privacy, one must consider the totality of the circumstances and consider the subject matter of the search, the affected person's interest in that subject matter, the person's subjective expectation of privacy, and the reasonableness of that expectation (para 18).

[174] With respect to the subject matter of the search, it is often important to look beyond the actual information that has been captured and consider what that information reveals. For example, in *Spencer*, Justice Cromwell found that the subject matter of the search went beyond the subscriber information that was obtained by the police and included the personal lifestyle details that could potentially be disclosed by that information (paras 25, 26). In effect, it allowed the police to correlate a person's name and address with activities that were of interest to state authorities; in that case, collection of child pornography. The subject matter of a search should

not be defined narrowly (*R v Reeves*, 2018 SCC 56 at para 29). This is particularly important when considering searches of electronic information (*R v Marakah*, 2017 SCC 59 at para 14).

[175] Similarly, the Supreme Court has held that the information obtained when a police dog sniffs a package is simply the odour emanating from it; but the dog's reaction to the smell permits an inference to be made about the contents of the package (see *R v Kang-Brown*, 2008 SCC 18). In determining the subject matter of a search, then, one must look beyond the information obtained to the inferences that could be drawn from it (*Marakah*, at para 20).

[176] Here, information about a person's [redacted] would allow the Service to draw inferences about that person's lifestyle and private activities. Individuals would have a direct interest in that subject matter and would subjectively expect that information to be kept private.

[177] In my view, that subjective expectation of privacy would be reasonable in the circumstances. Particularly significant in this context is the private nature of the information that can be inferred [redacted] The Service rightly points out that [redacted] will often reveal nothing about the owner of a device. For example, [redacted] may simply be [redacted] On the other hand, however, [redacted] may disclose the [redacted] with which the person of interest can be associated – [redacted] Typically, owners of devices have no control over [redacted] except possibly [redacted] This absence of control, however, does not mean that their expectation of privacy in the information that can be revealed is not reasonable (*Marakah* at para 41).

[178] Therefore, in my view, the information [redacted] may allow inferences to be drawn about lifestyle choices and private activities that individuals would wish to maintain and shield from state authorities (*R v Plant*, [1993] 3 SCR 281 at 293). Their expectation of privacy in that information is reasonable.

[179] Accordingly, given this difference between CSS operations, which involve minimally intrusive collections, and [redacted] surveys, which may involve collection of intrusive lifestyle information, I find that the latter require a warrant. These surveys may result in the gathering of personal information that is not open to public view and not released or abandoned by the targets of investigations. These factors tend in the direction of requiring a warrant (*R v Tessling*, 2004 SCC 67 at para 32).

[180] In addition, I have no evidence before me suggesting that it would be impracticable or infeasible to obtain a warrant to conduct [redacted] surveys (*Kang-Brown* at para 59).

[181] While I found that s 16 is a reasonable law to the extent that it permits conducting minimally intrusive searches without a warrant, I cannot come to the same conclusion regarding [redacted] surveys that collect personal lifestyle information. In my view, impartial judicial prior authorization – a warrant – is required for the Service to collect that information. In essence, I agree with Chief Justice Crampton when he found that "once [the Service] moves beyond minimally invasive collection activities, it will require a warrant" (at para 219).

V. Issue Four – Does s 16 authorize interception of communications outside Canada?

[182] The Service seeks an assurance that it has lawful authority to intercept [a foreign person's] communications from within Canada even if [the foreign person] is outside of Canada. The Service claims that this authority would enhance its ability to collect information relevant to the particular [redacted] capabilities, intentions, or activities.

[183] The issue arises because of the requirement in s 16 that foreign intelligence be collected only "within Canada." The words "within Canada" have been the subject of other litigation in this Court, most particularly in the case of *Re X (*[redacted]*)*, 2018 FC 738, affirmed in *Re X (*[redacted]*)* 2018 FCA 207. There, Justice Simon Noel concluded that the words "within Canada" in s 16 unambiguously mean within Canada's geographical boundaries (at paras 62, 100).

[184] The *amici* agree with the Service that the geographical requirements of s 16 are met when interceptions take place within Canada in respect of communications outside Canada.

[185] I agree. Still, to make clear what the Service proposes, I describe how these interceptions occur.

[186] A Service employee in charge of building software used in the collection of information from Communications Service Providers (CSPs), [redacted] explained how interceptions are made within Canada of communications outside Canada.

[187] The Service is able to conduct "telecom intercepts" of telephone communications, mobile device communications, and Internet activities [redacted]

[188] The Service refers to these interceptions as "Lawful Intercepts" or "LI" when conducted for purposes of protecting national security or assisting law enforcement pursuant to judicially-authorized warrants. [redacted]

[189] When a person leaves Canada, his or her phone will search for a suitable local service provider, one with which the person's Canadian CSP has entered into an agreement. This is commonly called "roaming." The foreign service provider will exchange information with the Canadian CSP in order to confirm that the person is a subscriber with a service plan.

[190] Accordingly, Canadian CSPs are aware when their customers leave the country and use their phones outside Canada. [redacted]

[redacted]

[191] [redacted]

[192] In the absence of clear legal authority permitting the Service to intercept a person's communications outside of Canada, the Service's current practice is to terminate an interception (their operation "goes down") if it becomes aware that [a foreign person] has left Canada. However, if [the foreign person] has left the country without the Service being aware, the interceptions will continue.

[193] Based on this evidence, I am satisfied that the Service's proposed interceptions will be made within Canada and will comply with the geographical limits of s 16. Essentially, the situation is analogous to domestic interceptions of foreign communications under s 12 as addressed comprehensively by Justice Richard Mosley in *X(Re)* 2009 FC 1058.

VI. Conclusion and Disposition

[194] This application provided an opportunity for the Court to receive from the Service detailed information about certain aspects of its foreign intelligence mandate under s 16 of the

CSIS Act. In particular, the Service explained its policies and practices relating to the incidental collection of information about Canadians, including elected officials, and to the pursuit of parallel s 16/s 12 operations. In both of these areas, I found the Service's conduct generally to be appropriate and satisfactory. However, I suggest that the Service should develop guidelines for distributing and unminimizing the identities of Canadians whose communications have been incidentally intercepted, and should provide the Court an opportunity to comment on them. It should also specifically disclose when there is a possibility that the communications of an elected official or other public servant may be intercepted, allowing the Court to impose any necessary terms and conditions on the execution of the warrants. Those terms and conditions could include imposing a requirement on the Service to return to the Court for directions on the handling of information collected.

[195] I also agree with the Service's proposed amendments to its s 16 warrant templates.

[196] I conclude that s 16 provides sufficient legal authority for the Service to carry out minimally intrusive searches to collect foreign intelligence. Use of CSS technology in the manner proposed by the Service falls into this category of searches and, therefore, does not require a warrant.

[197] However, I find that the interception of [redacted] data, to the extent that it captures a person's [redacted] is more than minimally intrusive. Having access to an individual's [redacted] would allow the Service to draw inferences about his or her personal

lifestyle choices [redacted] To comply with s 8 of the Charter, these searches require a judicially-authorized warrant.

[198] Finally, the Service's interception on Canadian soil of communications of [foreign persons] who are outside Canada complies with the geographical limitation in s 16. These interceptions occur "within Canada."

JUDGMENT in [redacted]

THIS COURT'S JUDGMENT is that:

1. The Service should develop guidelines for distributing and unminimizing the identities of Canadians whose communications have been incidentally intercepted under s 16, provide the Court an opportunity to comment on them, and specifically disclose to the Court when there is a possibility that the communications of an elected official or other public servant may be intercepted;

2. Section 16 provides sufficient legal authority for the use of CSS technology, in the manner proposed by the Service, without a warrant.

3. The interception of [redacted] data, to the extent that it captures a person's [redacted], is more than minimally intrusive and requires a warrant.

4. The Service's interception on Canadian soil of the communications of [foreign persons] who are outside Canada complies with the geographical limitation in s 16 as they occur "within Canada."

5. Counsel for the Attorney General of Canada shall, within 15 days, make suggestions for information in this decision that should be redacted before it is released publicly. The *amicus* shall have 15 days from the receipt of those suggestions to make submissions on them. It is understood that counsel shall make every effort to keep redactions to a minimum.

"James W. O'Reilly"
Judge

ANNEX

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

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

Canada or a foreign state, and	ou idéologique au Canada ou dans un État étranger;
(*d*) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada,	*d*) les activités qui, par des actions cachées et illicites, visent à saper le régime de gouvernement constitutionnellement établi au Canada ou dont le but immédiat ou ultime est sa destruction ou son renversement, par la violence.
but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (*a*) to (*d*).	La présente définition ne vise toutefois pas les activités licites de défense d'une cause, de protestation ou de manifestation d'un désaccord qui n'ont aucun lien avec les activités mentionnées aux alinéas *a*) à *d*).
…	[…]
DUTIES AND FUNCTIONS OF SERVICE	FONCTIONS DU SERVICE
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.
(2) For greater certainty, the Service may perform its duties	(2) Il est entendu que le Service peut exercer les

and functions under subsection (1) within or outside Canada.

fonctions que le paragraphe (1) lui confère même à l'extérieur 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.

(2) The measures shall be reasonable and proportional in the circumstances, having regard to the nature of the threat, the nature of the measures and the reasonable availability of other means to reduce the threat.

(2) Les mesures doivent être justes et adaptées aux circonstances, compte tenu de la nature de la menace et des mesures, ainsi que des solutions de rechange acceptables pour réduire la menace.

(3) The Service shall not take measures to reduce a threat to the security of Canada if those measures will contravene a right or freedom guaranteed by the *Canadian Charter of Rights and Freedoms* or will be contrary to other Canadian law, unless the Service is authorized to take them by a warrant issued under section 21.1.

(3) La prise par le Service de mesures pour réduire une menace envers la sécurité du Canada est subordonnée à l'obtention d'un mandat au titre de l'article 21.1 s'il s'agit de mesures qui porteront atteinte à un droit ou à une liberté garantis par la *Charte canadienne des droits et libertés* ou qui seront contraires à d'autres règles du droit canadien.

(4) For greater certainty, nothing in subsection (1) confers on the Service any law enforcement power.

(4) Il est entendu que le paragraphe (1) ne confère au Service aucun pouvoir de contrôle d'application de la loi.

12.2 (1) In taking measures to reduce a threat to the

12.2 (1) Dans le cadre des mesures qu'il prend pour réduire une menace envers la

security of Canada, the Service shall not

(*a*) cause, intentionally or by criminal negligence, death or bodily harm to an individual;

(*b*) wilfully attempt in any manner to obstruct, pervert or defeat the course of justice; or

(*c*) violate the sexual integrity of an individual.

(2) In subsection (1), "bodily harm" has the same meaning as in section 2 of the *Criminal Code*.

…

16. (1) Subject to this section, the Service may, in relation to the defence of Canada or the conduct of the international affairs of Canada, assist the Minister of National Defence or the Minister of Foreign Affairs, within Canada, in the collection of information or intelligence relating to the capabilities, intentions or activities of

(*a*) any foreign state or group of foreign states; or

sécurité du Canada, le Service ne peut :

a) causer, volontairement ou par négligence criminelle, des lésions corporelles à un individu ou la mort de celui-ci;

b) tenter volontairement de quelque manière d'entraver, de détourner ou de contrecarrer le cours de la justice;

c) porter atteinte à l'intégrité sexuelle d'un individu.

(2) Au paragraphe (1), « lésions corporelles » s'entend au sens de l'article 2 du *Code criminel*.

[…]

16. (1) Sous réserve des autres dispositions du présent article, le Service peut, dans les domaines de la défense et de la conduite des affaires internationales du Canada, prêter son assistance au ministre de la Défense nationale ou au ministre des Affaires étrangères, dans les limites du Canada, à la collecte d'informations ou de renseignements sur les moyens, les intentions ou les activités :

a) d'un État étranger ou d'un groupe d'États étrangers;

(*b*) any person other than	*b*) d'une personne qui n'appartient à aucune des catégories suivantes :
(i) a Canadian citizen,	(i) les citoyens canadiens,
(ii) a permanent resident within the meaning of subsection 2(1) of the *Immigration and Refugee Protection Act*, or	(ii) les résidents permanents au sens du paragraphe 2(1) de la *Loi sur l'immigration et la protection des réfugiés*,
(iii) a corporation incorporated by or under an Act of Parliament or of the legislature of a province.	(iii) les personnes morales constituées sous le régime d'une loi fédérale ou provinciale.
(2) The assistance provided pursuant to subsection (1) shall not be directed at any person referred to in subparagraph (1)(*b*)(i), (ii) or (iii).	(2) L'assistance autorisée au paragraphe (1) est subordonnée au fait qu'elle ne vise pas des personnes mentionnées à l'alinéa (1)*b*).
(3) The Service shall not perform its duties and functions under subsection (1) unless it does so	(3) L'exercice par le Service des fonctions visées au paragraphe (1) est subordonné :
(*a*) on the personal request in writing of the Minister of National Defence or the Minister of Foreign Affairs; and	*a*) à une demande personnelle écrite du ministre de la Défense nationale ou du ministre des Affaires étrangères;
(*b*) with the personal consent in writing of the Minister.	*b*) au consentement personnel écrit du ministre.
…	[…]
PART II JUDICIAL CONTROL	PARTIE II CONTRÔLE JUDICIAIRE

21. (1) If the Director or any employee designated by the Minister for the purpose believes, on reasonable grounds, that a warrant under this section is required to enable the Service to investigate, within or outside Canada, a threat to the security of Canada or to perform its duties and functions under section 16, the Director or employee may, after having obtained the Minister's approval, make an application in accordance with subsection (2) to a judge for a warrant under this section.

21. (1) Le directeur ou un employé désigné à cette fin par le ministre peut, après avoir obtenu l'approbation du ministre, demander à un juge de décerner un mandat en conformité avec le présent article s'il a des motifs raisonnables de croire que le mandat est nécessaire pour permettre au Service de faire enquête, au Canada ou à l'extérieur du Canada, sur des menaces envers la sécurité du Canada ou d'exercer les fonctions qui lui sont conférées en vertu de l'article 16.

(2) An application to a judge under subsection (1) shall be made in writing and be accompanied by an affidavit of the applicant deposing to the following matters, namely,

(2) La demande visée au paragraphe (1) est présentée par écrit et accompagnée de l'affidavit du demandeur portant sur les points suivants :

(*a*) the facts relied on to justify the belief, on reasonable grounds, that a warrant under this section is required to enable the Service to investigate a threat to the security of Canada or to perform its duties and functions under section 16;

a) les faits sur lesquels le demandeur s'appuie pour avoir des motifs raisonnables de croire que le mandat est nécessaire aux fins visées au paragraphe (1);

(*b*) that other investigative procedures have been tried and have failed or why it appears that they are unlikely to succeed, that the urgency of the matter is such that it would be impractical to carry out the investigation using only

b) le fait que d'autres méthodes d'enquête ont été essayées en vain, ou la raison pour laquelle elles semblent avoir peu de chances de succès, le fait que l'urgence de l'affaire est telle qu'il serait très difficile de mener

other investigative procedures or that without a warrant under this section it is likely that information of importance with respect to the threat to the security of Canada or the performance of the duties and functions under section 16 referred to in paragraph (*a*) would not be obtained;

l'enquête sans mandat ou le fait que, sans mandat, il est probable que des informations importantes concernant les menaces ou les fonctions visées au paragraphe (1) ne pourraient être acquises;

(*c*) the type of communication proposed to be intercepted, the type of information records, documents or things proposed to be obtained and the powers referred to in paragraphs (3)(*a*) to (*c*) proposed to be exercised for that purpose;

c) les catégories de communications dont l'interception, les catégories d'informations, de documents ou d'objets dont l'acquisition, ou les pouvoirs visés aux alinéas (3)*a*) à *c*) dont l'exercice, sont à autoriser;

(*d*) the identity of the person, if known, whose communication is proposed to be intercepted or who has possession of the information, record, document or thing proposed to be obtained;

d) l'identité de la personne, si elle est connue, dont les communications sont à intercepter ou qui est en possession des informations, documents ou objets à acquérir;

(*e*) the persons or classes of persons to whom the warrant is proposed to be directed;

e) les personnes ou catégories de personnes destinataires du mandat demandé;

(*f*) a general description of the place where the warrant is proposed to be executed, if a general description of that place can be given;

f) si possible, une description générale du lieu où le mandat demandé est à exécuter;

(*g*) the period, not exceeding sixty days or one year, as the case may

g) la durée de validité applicable en vertu du paragraphe (5), de soixante

be, for which the warrant is requested to be in force that is applicable by virtue of subsection (5); and	jours ou d'un an au maximum, selon le cas, demandée pour le mandat;
(*h*) any previous application made under subsection (1) in relation to a person who is identified in the affidavit in accordance with paragraph (*d*), the date on which each such application was made, the name of the judge to whom it was made and the judge's decision on it.	*h*) la mention des demandes antérieures présentées au titre du paragraphe (1) touchant des personnes visées à l'alinéa *d*), la date de chacune de ces demandes, le nom du juge à qui elles ont été présentées et la décision de celui-ci dans chaque cas.
(3) Notwithstanding any other law but subject to the *Statistics Act*, where the judge to whom an application under subsection (1) is made is satisfied of the matters referred to in paragraphs (2)(*a*) and (*b*) set out in the affidavit accompanying the application, the judge may issue a warrant authorizing the persons to whom it is directed to intercept any communication or obtain any information, record, document or thing and, for that purpose,	(3) Par dérogation à toute autre règle de droit mais sous réserve de la *Loi sur la statistique*, le juge à qui est présentée la demande visée au paragraphe (1) peut décerner le mandat s'il est convaincu de l'existence des faits mentionnés aux alinéas (2)*a*) et *b*) et dans l'affidavit qui accompagne la demande; le mandat autorise ses destinataires à intercepter des communications ou à acquérir des informations, documents ou objets. À cette fin, il peut autoriser aussi, de leur part :
(*a*) to enter any place or open or obtain access to any thing;	*a*) l'accès à un lieu ou un objet ou l'ouverture d'un objet;
(*b*) to search for, remove or return, or examine, take extracts from or make copies of or record in any other manner the information, record, document or thing; or	*b*) la recherche, l'enlèvement ou la remise en place de tout document ou objet, leur examen, le prélèvement des informations qui s'y trouvent, ainsi que leur

enregistrement et l'établissement de copies ou d'extraits par tout procédé;

(*c*) to install, maintain or remove any thing.

c) l'installation, l'entretien et l'enlèvement d'objets.

(3.1) Without regard to any other law, including that of any foreign state, a judge may, in a warrant issued under subsection (3), authorize activities outside Canada to enable the Service to investigate a threat to the security of Canada.

(3.1) Sans égard à toute autre règle de droit, notamment le droit de tout État étranger, le juge peut autoriser l'exercice à l'extérieur du Canada des activités autorisées par le mandat décerné, en vertu du paragraphe (3), pour permettre au Service de faire enquête sur des menaces envers la sécurité du Canada.

(4) There shall be specified in a warrant issued under subsection (3)

(4) Le mandat décerné en vertu du paragraphe (3) porte les indications suivantes :

(*a*) the type of communication authorized to be intercepted, the type of information, records, documents or things authorized to be obtained and the powers referred to in paragraphs (3)(*a*) to (*c*) authorized to be exercised for that purpose;

a) les catégories de communications dont l'interception, les catégories d'informations, de documents ou d'objets dont l'acquisition, ou les pouvoirs visés aux alinéas (3)*a*) à *c*) dont l'exercice, sont autorisés;

(*b*) the identity of the person, if known, whose communication is to be intercepted or who has possession of the information, record, document or thing to be obtained;

b) l'identité de la personne, si elle est connue, dont les communications sont à intercepter ou qui est en possession des informations, documents ou objets à acquérir;

(*c*) the persons or classes of persons to whom the warrant is directed;

c) les personnes ou catégories de personnes destinataires du mandat;

(*d*) a general description of the place where the warrant may be executed, if a general description of that place can be given;

d) si possible, une description générale du lieu où le mandat peut être exécuté;

(*e*) the period for which the warrant is in force; and

e) la durée de validité du mandat;

(*f*) such terms and conditions as the judge considers advisable in the public interest.

f) les conditions que le juge estime indiquées dans l'intérêt public.

(5) A warrant shall not be issued under subsection (3) for a period exceeding

(5) Il ne peut être décerné de mandat en vertu du paragraphe (3) que pour une période maximale :

(*a*) sixty days where the warrant is issued to enable the Service to investigate a threat to the security of Canada within the meaning of paragraph (*d*) of the definition of that expression in section 2; or

a) de soixante jours, lorsque le mandat est décerné pour permettre au Service de faire enquête sur des menaces envers la sécurité du Canada au sens de l'alinéa *d*) de la définition de telles menaces contenue à l'article 2;

(*b*) one year in any other case.

b) d'un an, dans tout autre cas.

21.1 (1) If the Director or any employee who is designated by the Minister for the purpose believes on reasonable grounds that a warrant under this section is required to enable the Service to take measures, within or outside Canada, to reduce a

21.1 (1) Le directeur ou un employé désigné à cette fin par le ministre peut, après avoir obtenu l'approbation du ministre, demander à un juge de décerner un mandat en conformité avec le présent article s'il a des motifs raisonnables de croire que le

threat to the security of Canada, the Director or employee may, after having obtained the Minister's approval, make an application in accordance with subsection (2) to a judge for a warrant under this section.

mandat est nécessaire pour permettre au Service de prendre, au Canada ou à l'extérieur du Canada, des mesures pour réduire une menace envers la sécurité du Canada.

(2) An application to a judge under subsection (1) shall be made in writing and be accompanied by the applicant's affidavit deposing to the following matters:

(2) La demande est présentée par écrit et accompagnée de l'affidavit du demandeur portant sur les points suivants :

(*a*) the facts relied on to justify the belief on reasonable grounds that a warrant under this section is required to enable the Service to take measures to reduce a threat to the security of Canada;

a) les faits sur lesquels le demandeur s'appuie pour avoir des motifs raisonnables de croire que le mandat est nécessaire pour permettre au Service de prendre des mesures pour réduire une menace envers la sécurité du Canada;

(*b*) the measures proposed to be taken;

b) les mesures envisagées;

(*c*) the reasonableness and proportionality, in the circumstances, of the proposed measures, having regard to the nature of the threat, the nature of the measures and the reasonable availability of other means to reduce the threat;

c) le fait que les mesures envisagées sont justes et adaptées aux circonstances, compte tenu de la nature de la menace et des mesures, ainsi que des solutions de rechange acceptables pour réduire la menace;

(*d*) the identity of the persons, if known, who are directly affected by the proposed measures;

d) l'identité des personnes qui sont touchées directement par les mesures envisagées, si elle est connue;

(*e*) the persons or classes of persons to whom the warrant is proposed to be directed;

e) les personnes ou catégories de personnes destinataires du mandat demandé;

(*f*) a general description of the place where the warrant is proposed to be executed, if a general description of that place can be given;

f) si possible, une description générale du lieu où le mandat demandé est à exécuter;

(*g*) the period, not exceeding 60 days or 120 days, as the case may be, for which the warrant is requested to be in force that is applicable by virtue of subsection (6); and

g) la durée de validité applicable en vertu du paragraphe (6), de soixante jours ou de cent vingt jours au maximum, selon le cas, demandée pour le mandat;

(*h*) any previous application made under subsection (1) in relation to a person who is identified in the affidavit in accordance with paragraph (*d*), the date on which each such application was made, the name of the judge to whom it was made and the judge's decision on it.

h) la mention des demandes antérieures présentées au titre du paragraphe (1) touchant des personnes visées à l'alinéa *d*), la date de chacune de ces demandes, le nom du juge à qui elles ont été présentées et la décision de celui-ci dans chaque cas.

(3) Despite any other law but subject to the *Statistics Act*, if the judge to whom an application under subsection (1) is made is satisfied of the matters referred to in paragraphs (2)(*a*) and (*c*) that are set out in the affidavit accompanying the application, the judge may issue a warrant authorizing the persons to whom it is directed to take the measures specified in it and, for that purpose,

(3) Par dérogation à toute autre règle de droit mais sous réserve de la *Loi sur la statistique*, le juge à qui est présentée la demande visée au paragraphe (1) peut décerner le mandat s'il est convaincu de l'existence des faits qui sont mentionnés aux alinéas (2)*a*) et *c*) et énoncés dans l'affidavit qui accompagne la demande; le mandat autorise ses destinataires à prendre les mesures qui y sont indiquées. À cette fin, il peut autoriser aussi, de leur part :

(*a*) to enter any place or open or obtain access to any thing;	*a*) l'accès à un lieu ou un objet ou l'ouverture d'un objet;
(*b*) to search for, remove or return, or examine, take extracts from or make copies of or record in any other manner the information, record, document or thing;	*b*) la recherche, l'enlèvement ou la remise en place de tout document ou objet, leur examen, le prélèvement des informations qui s'y trouvent, ainsi que leur enregistrement et l'établissement de copies ou d'extraits par tout procédé;
(*c*) to install, maintain or remove any thing; or	*c*) l'installation, l'entretien et l'enlèvement d'objets;
(d) to do any other thing that is reasonably necessary to take those measures.	d) les autres actes nécessaires dans les circonstances à la prise des mesures.
(4) Without regard to any other law, including that of any foreign state, a judge may, in a warrant issued under subsection (3), authorize the measures specified in it to be taken outside Canada.	(4) Sans égard à toute autre règle de droit, notamment le droit de tout État étranger, le juge peut autoriser la prise à l'extérieur du Canada des mesures indiquées dans le mandat décerné en vertu du paragraphe (3).
(5) There shall be specified in a warrant issued under subsection (3)	(5) Le mandat décerné en vertu du paragraphe (3) porte les indications suivantes :
(*a*) the measures authorized to be taken;	*a*) les mesures autorisées;
(*b*) the identity of the persons, if known, who are directly affected by the measures;	*b*) l'identité des personnes qui sont touchées directement par les mesures, si elle est connue;

(*c*) the persons or classes of persons towhom the warrant is directed;	*c*) les personnes ou catégories de personnes destinataires du mandat;
(*d*) a general description of the place where the warrant may be executed, if a general description of that place can be given;	*d*) si possible, une description générale du lieu où le mandat peut être exécuté;
(*e*) the period for which the warrant is in force; and	*e*) la durée de validité du mandat;
(*f*) any terms and conditions that the judge considers advisable in the public interest.	*f*) les conditions que le juge estime indiquées dans l'intérêt public.
(6) A warrant shall not be issued under subsection (3) for a period exceeding	(6) Il ne peut être décerné de mandat en vertu du paragraphe (3) que pour une période maximale :
(*a*) 60 days if the warrant is issued to enable the Service to take measures to reduce a threat to the security of Canada within the meaning of paragraph (*d*) of the definition "threats to the security of Canada" in section 2; or	*a*) de soixante jours, lorsque le mandat est décerné pour permettre au Service de prendre des mesures pour réduire une menace envers la sécurité du Canada au sens de l'alinéa *d*) de la définition de telles menaces à l'article 2;
(*b*) 120 days in any other case.	*b*) de cent vingt jours, dans tout autre cas.

FEDERAL COURT

SOLICITORS OF RECORD

DOCKET:	[redacted]
STYLE OF CAUSE:	IN THE MATTER OF AN APPLICATION BY [redacted] FOR WARRANTS PURSUANT TO SECTIONS 16 AND 21 OF THE *CANADIAN SECURITY INTELLIGENCE SERVICES ACT*, RSC 1985, c. C-23 AND IN THE MATTER OF [A FOREIGN STATE, GROUP OF STATES, CORPORATION, OR PERSON]
PLACE OF HEARING:	OTTAWA, ONTARIO
DATE OF HEARING:	MARCH 15, 2018, MARCH 16, 2018 MARCH 20, 2018 APRIL 24, 2018 JULY 11, 2018
JUDGMENT AND REASONS:	O'REILLY J.
DATED:	JUNE 16, 2020
AMENDED	MARCH 09, 2022

APPEARANCES:

Ms. Jennifer Poirier Ms. Amy Joslin-Besner	FOR THE APPLICANT ATTORNEY GENERAL OF CANADA
Mr. Gord Cameron	*AMICUS CURIAE*
Mr. Owen Rees	*AMICUS CURIAE*

SOLICITORS OF RECORD:

Deputy Attorney General of Canada Ottawa, Ontario	FOR THE APPLICANT ATTORNEY GENERAL OF CANADA
Blakes Law Firm Conway Baxter LLP	*AMICUS CURIAE*