Federal Court  Cour fédérale

TOP SECRET

Date: 20170927

Dockets: CONF-3-17

Citation Number: 2017 FC 1048

Ottawa, Ontario, September 27, 2017

PRESENT: THE CHIEF JUSTICE

Docket: [redacted]

BETWEEN:

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

and

IN THE MATTER OF [redacted] THREAT-RELATED ACTIVITIES

and

Docket: [redacted]

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

and

IN THE MATTER OF ISLAMIST TERRORISM

PUBLIC JUDGMENT AND REASONS

I. Introduction

[1] These applications concern requests by the Canadian Security Intelligence Service [CSIS] for warrants in relation to its investigation of two separate groups of activities that I am satisfied may on reasonable grounds be suspected of constituting threats to the security of Canada.

CSIS has defined the first group in terms of "Islamist terrorism." Those activities are the focus of the application in Court file [redacted] The second group consists of certain activities engaged in by [redacted] Those activities are described in materials filed by CSIS in Court file [redacted]

[2] The applications raise three issues pertaining to CSIS's request to be able to obtain basic identifying information [BII] from communications services providers [CSPs]. That information would be obtained in respect of communications accounts of individuals whose telephone number, [redacted] or other electronic identifiers may in the future come to CSIS's attention in the course of its investigations of the activities described above. BII consists of the name and address of a subscriber to a communications account, [redacted]

[redacted] [The information relating to IP addresses in certain circumstances]

[redacted]

[3] The Attorney General concedes that in the absence of judicial pre-authorization, CSIS cannot obtain BII in respect of a person's communications account without contravening that person's right to be secure against unreasonable search or seizure, pursuant to section 8 of the *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [the *Charter*].

[4] Accordingly, the focus of these applications has been upon a broad BII authorization that CSIS is seeking in each of [redacted] and [redacted], a narrower BII authorization that it is seeking in [redacted] alone, and a delegation issue that exists with respect to the first of those

two authorizations. More specifically, the three issues raised by these applications are as follows:

i. Can the Court authorize CSIS to obtain BII in respect of communications accounts corresponding to telephone numbers or electronic identifiers that *may in the future* come to its attention in the course of its investigations, where CSIS has not described and established their specific nexus to those investigations? (This is a common issue in both applications.)

ii. Can the Court authorize CSIS to obtain BII in respect of communications accounts identified pursuant to its review of specifically defined information obtained in relation to [redacted] named individuals and [redacted] additional individuals who have been identified by [redacted] (This issue arises only in [redacted]

iii. Can the Court authorize an employee of CSIS to obtain BII in respect of a communications account that corresponds to a telephone number or an electronic identifier, where a "Chief" within CSIS determines that the account was identified during its investigation, and that the BII would assist CSIS in its investigation? (This is a common issue in both applications.)

[5] In my view, the Court cannot provide the first of the requested authorizations described above. It does not meet the basic requirements for authorizing intrusive activity by the state.

[6] Before the Court may authorize CSIS to obtain BII or to exercise other intrusive search powers, the Court must have an understanding of the nexus between CSIS's investigation and the specific persons or class of persons whose privacy rights would be engaged. Only then can the Court assess whether the specific privacy interests of those persons must give way to the interests of the state in obtaining the information in question. In addition, CSIS must satisfy the requirements for obtaining a warrant set forth in subsections 21(2) and (3) of the *Canadian Security Intelligence Service Act*, RSC 1985, c C-23 [the Act], in respect of such person or class of persons.

[7] The Court has not been provided with that required understanding of the nexus described above in respect of the broad BII authorization that CSIS is seeking in both [redacted] and [redacted] Indeed, the Court has not been provided with any sense whatsoever as to how the individual or class of individuals whose privacy interests would be intruded upon would be linked to its investigations.

[8] With respect to the second, narrower, BII authorization that CSIS has requested in [redacted] alone, I am satisfied that the required nexus has been described and established by CSIS. This is because that authorization is confined to telephone numbers or electronic identifiers that CSIS may identify in the course of reviewing information that specifically relates to [redacted] identified individuals who are subjects of investigation. [redacted] of those individuals have been identified by name, while the remaining [redacted] have been identified by reference to [redacted]

[9] The information that relates to those individuals includes BII [redacted] information will reveal the [redacted] identifiers [redacted]

[10] I am satisfied that there are reasonable grounds to believe that anyone with whom those [redacted] individuals has been in contact may be able to provide information that will assist CSIS to advance its investigation into the threat-related activities [redacted] that it has identified. For this reason, I am satisfied that there are reasonable grounds to believe that CSIS requires the BII relating to the communications accounts that correspond to the telephone numbers and electronic identifiers of those third parties, to advance its investigation. Without being able to obtain that BII, [redacted]

[11] Although the Court has not been provided with the names of [redacted] of those individuals, the Court has been provided with sufficient information regarding [redacted] to be able to conduct the assessment required by section 8 of the *Charter*. That assessment is whether the specific privacy interests of those individuals must give way to the interests of the state in obtaining the BII that CSIS requires to advance its investigation into the identified threat-related activities [redacted]

[12] At the time it issues a warrant authorizing the exercise of powers that would intrude upon the privacy interests of one or more individuals or classes of persons, the Court does not need to

know the specific names of those individuals or persons within the class. However, the Court needs to have a sufficient understanding of the nexus between CSIS's investigation and the specific persons or class of persons whose privacy interests would be intruded upon. The Court has been provided with that understanding in respect of the [redacted] individuals [redacted] have been described to the Court, as well as in respect of the third parties who CSIS may discover have been in contact with those individuals, or with the [redacted] other individuals who have been identified by name.

[13] Where the Court is not able to conduct, in advance, the assessment required by section 8 of the *Charter* in respect of the specific individuals or class of individuals whose privacy interests would be engaged by CSIS's access to their BII, CSIS will need to return to the Court each time it identifies additional telephone numbers or electronic identifiers in respect of which it wishes to obtain BII from a CSP. At that time, CSIS will have to establish a sufficient nexus between the telephone number or other identifier in question and its investigations to satisfy the Court that there are reasonable grounds to believe that CSIS requires the BII of the corresponding communications account to advance those investigations.

[14] The third issue raised in these proceedings is whether the Court can authorize any employee of CSIS to obtain BII in respect of a communications account, where an individual holding the position of Chief within CSIS makes certain determinations. In my view, the Court cannot do so, because this would amount to the delegation of functions that must be exercised by the Court itself. Although the Court may delegate to CSIS certain types of decisions with respect to the execution of its warrants, it cannot delegate the determination of which specific

communications accounts will be the subject of requests to CSPs for BII. To the extent that this determination requires an assessment of whether the privacy interests of the persons in question must give way to the interests of CSIS in obtaining the BII in question, this is a function that must be performed by the Court.

[15] I recognize that the conclusions I have reached in respect of the first and third issues discussed above may well impose a potentially significant additional burden on CSIS. I also recognize that this may give rise to additional costs and delays associated with obtaining BII authorizations in relation to telephone numbers or electronic identifiers that may come to CSIS's attention during the course of its investigations into Islamist terrorism and the threat-related activities [redacted] Given the adverse implications that the potential delays, in particular, may have for CSIS's ability to investigate threat-related activities, the Court will remain open to considering alternate approaches that are *Charter* compliant.

[16] These reasons for judgment are being issued contemporaneously with my reasons for judgment in [redacted] which concerns CSIS's use of cellular-site simulator [CSS] technology to capture the identifying characteristics of an individual's mobile device(s) without a warrant [redacted]

II. Background

[17] This Court has been authorizing CSIS to obtain subscriber and similar information from CSPs in respect of accounts corresponding to telephone numbers and electronic identifiers for many years. In most cases, such authorizations have been provided in respect of the [redacted] identifiers of known individuals who are subjects of investigation, or of third parties with whom such individuals may communicate. However, in some cases the Court has also authorized CSIS to obtain such information in respect of communications accounts of known, but still unidentified, individuals. For example, such authorizations have been provided in respect of individuals [redacted] The same is true with respect to the [redacted] identifiers of third parties with whom such known, but as yet unidentified, individuals have communicated, or may in the future communicate. Given that the [redacted] identifiers in question are not yet known at the time of the warrant application, they cannot be specified in the warrant.

[18] The types of authorizations described above have always been provided in warrants that have focused primarily upon named subjects of investigation, also known as "targets," and their involvement in particular threat-related activities. In some of those warrants, the Court also granted authorizations to obtain BII in relation to the communication accounts associated with [redacted] identifiers that CSIS identified during its investigation of the threat to the security of Canada in question, even where there was no direct link between such [redacted] identifiers and the target(s) identified in the warrants. There was

simply the indirect link that existed by virtue of the fact that the [redacted] identifier would be identified in the future course of CSIS's investigation of the same threat to the security of Canada with which the named targets were also connected.

[19] However, beginning in 2013, some of my colleagues and I started to express concerns about granting the latter type of authorizations. After CSIS failed to avail itself of opportunities to address our concerns, we began to narrow the scope of the powers that we authorized. However, given that we did so in the context of individual applications for warrants, which sometimes had to be dealt with on an urgent basis, this gave rise to some inconsistencies in the language of the authorizations in question.

[20] As a result of the foregoing, Justice Noël advised CSIS in *X (Re)*, 2016 FC 1105, at para 230 [*X (Re)*], that broad authorizations of the type being sought in the present proceedings, as well as authorizations to obtain [redacted] would no longer be granted by the Court until they were the subject of further exchanges between the Court and CSIS. Soon afterwards, in [redacted] I requested that CSIS endeavour to establish the legal basis for this Court to authorize such powers, in a separate proceeding. I explained that if CSIS could establish that legal basis, the powers in question could be authorized in a single application that would be made each year. Among other things, I considered that such an approach would avoid having to deal with CSIS's requests for such broad authorizations in the context of multiple different applications made over the course of a year, that are otherwise focused on named subjects of investigation. I made the foregoing request after declining to issue such an authorization.

[21] The application in [redacted] is CSIS's response to my request and to Justice Noël's decision. CSIS requested that I hear that application.

[22] Given the position taken by Justice Noël in *X (Re)* with respect to broad authorizations to obtain access to subscriber data, CSIS's application in [redacted] was separated into two phases. The first phase focused on warrant powers that CSIS sought in respect of individuals who are subjects of its investigation into the threat to the security of Canada posed by [redacted] That phase of the proceeding took place in February of this year, and was based on affidavit evidence provided by Mr. [redacted] After being satisfied that [redacted] is engaged in activities that may on reasonable grounds be suspected of constituting threats to the security of Canada, Justice Noël issued the warrants that were sought at that time.

[23] At Justice Noël's suggestion, the second phase of [redacted] took place before me, and concerned two additional authorizations that CSIS is seeking to add to three of the warrants that Justice Noël issued in the initial phase of that proceeding. The first of those authorizations is essentially the same as the sole, and very broad, authorization being sought in [redacted] [the BII Warrant]. The second is much more focused, and would enable CSIS to obtain the BII corresponding to the communications accounts of third parties whose telephone number or electronic identifier has been linked to one or more of [redacted] named individuals, or to [redacted] unnamed individuals [redacted] At CSIS's suggestion, the evidentiary hearings and oral submissions in this second phase of [redacted] as well as in [redacted] were held separately, but concurrently, on [redacted] and [redacted] of this year.

[24] To preserve the *status quo* with respect to the BII-type power that is being sought in [redacted] in relation to the threat to the security of Canada posed by Islamist terrorism, I granted an interim order on [redacted] which provided CSIS with that authorization for 60 days, to permit me to complete this decision.[1]

[25] In view of the nature of the legal issues raised in this application, the Court retained Mr. Gordon Cameron and Mr. Owen Rees to act as *amici curiae*.

[26] Given that BII authorizations similar to those being requested in these applications may be sought in future proceedings before other designated judges of this Court, I considered it appropriate to convene the designated judges of the Court to join me on the bench, so that they would have the benefit of the evidence provided by the affiants, including on cross-examination by the *Amici*. I also considered it to be important that they have the benefit of responses provided by the affiants to questions that any of them, or I, might pose. This should assist each of the designated judges of the Court in any future applications that may involve a request for a BII or similar authorization, and could reduce the need for similar evidence in those applications.

[27] Notwithstanding the involvement of other designated judges of this Court in this proceeding, I assured CSIS and representatives of the Attorney General at the outset of the initial hearing on these applications that my judicial independence would not thereby be compromised in any way. I, and I alone, have decided the issues that have been raised in these applications.

---

[1] The last warrant that contained the BII authorization in respect of CSIS's investigation into [redacted]

[28] Like several of my designated colleagues before me in previous applications dating back several years, I am satisfied that there are reasonable grounds to believe that activities that CSIS has defined as "Islamist terrorism" constitute a threat to the security of Canada, and that the same is true with respect to the threat-related activities engaged in by [redacted] that CSIS has identified.

[29] Accordingly, the balance of these reasons for judgment will focus on the three issues that are identified at paragraph 4 above.

[30] In passing, and for completeness, I will add that CSIS informed the Court earlier this year that it did not intend to seek or address in either [redacted] or [redacted] the [redacted] that was referred to in *X (Re)*, above. The Court understands that CSIS may return to the Court to make separate submissions in respect of that power at a future date, and that CSIS will not in the meantime be seeking any authorizations to use that power in respect of [redacted] communications accounts that correspond to telephone numbers or electronic identifiers that have no direct nexus with identified subjects of investigation.

III. The BII Authorizations Requested by CSIS

[31] The warrant that CSIS has requested the Court to issue in [redacted] consists of a single authorization. It is as follows:

> I authorize the Director and any employee of the service acting under his authority to obtain BII relating to any account with a CSP where a Chief determines that

a) the account was identified during the investigation of Islamist terrorism and

b) the identity of the subscriber to the account will assist in the investigation of Islamist terrorism.

[32] "BII" is defined in the warrant to mean:

i. The name of a subscriber to an account;

ii. The subscriber's address;

[The information relating to IP addresses in certain circumstances]

[33] In essence, this authorization would enable CSIS to obtain BII in respect of any communications account corresponding to any telephone number or electronic identifier that CSIS may identify during its investigation into Islamist terrorism, where a Chief within CSIS determines that BII will assist CSIS to advance its investigation.

[34] The Attorney General analogizes this authorization to a power to obtain "telephone book" information, which traditionally has been required to identify individuals. The Attorney General, the affiant in [redacted] and the affiant in [redacted] each maintained that this was the sole purpose of the BII authorization being requested. In this regard, they emphasized that the BII authorization is not used to track online activity. The Attorney General added that if CSIS wanted to exercise such a power or indeed any other

intrusive powers in respect of a person, it would have to return to the Court to seek specific authorizations to do so.

[35] The BII Warrant that has been requested in [redacted] also provides that if, in executing the warrant, CSIS provides [redacted] CSIS shall also provide [redacted] Islamist terrorism. This requirement has been included as a safeguard to help ensure that BII is provided in respect of the correct account, [redacted]

[36] For the purposes of the BII Warrant, "Islamist terrorism" is defined to mean "activities in paragraph (c) of the definition of 'threats to the security of Canada' found in section 2 of the Act [redacted] including activities of the [redacted]

[37] Both Mr. [redacted] and Mr. [redacted] testified that an authorization to obtain BII is crucial to CSIS's ability to investigate the threats to the security of Canada posed by the activities [redacted] and Islamist terrorism. This is because this may be the only manner in which CSIS can identify a person who is behind a phone number [or an electronic identifier] [redacted] In addition, the ability to identify individuals and assess the nature of their relationship to Islamist terrorism or to the threat related activities [redacted] is a fundamental building block of an investigation. This is particularly so given that many people associated with the threats in

question interact exclusively or primarily by electronic means, and may never meet in person. According to Mr. [redacted] "identification is [redacted] part of the job," and [redacted] He emphasized that, without being able to identify someone, CSIS would not be able to fulfill its mandate.

[38] According to Mr. [redacted] the 2014-2016 Intelligence Priorities for CSIS from the Minister of Public Safety [redacted]

[39] The BII authorizations that CSIS is seeking in the amendments that it has requested be made to three of the warrants were issued in the first phase of [redacted] are of two types. The first type would provide essentially the same broad power that is being sought in [redacted] That is to say, it would provide essentially the same authorization as is being requested in the BII Warrant, albeit in respect of communications accounts that are identified during CSIS's investigation of the threat-related activities [redacted] that it has described.

[40] The second type of authorization that CSIS is seeking to add to three of the warrants that have been issued in [redacted] is much narrower. In brief, it would authorize CSIS to obtain BII in respect of communications accounts identified pursuant to its review of specifically defined information obtained in relation to [redacted] named individuals and [redacted] additional individuals who [redacted]

[41] It bears underscoring that no individuals are named in the BII Warrant being sought in [redacted] or in the first group of amendments that CSIS is seeking to add to three of the warrants that have been issued in [redacted] In the words of Mr. [redacted] "the warrant itself is not [redacted] it's against Islamist terrorism." Likewise, the amendments sought to three of the warrants issued in [redacted] are directed towards the threat-related activities [redacted].

IV. Issues

[42] As explained at paragraph 4 above, the applications in [redacted] and [redacted] raise the following three issues:

i. Can the Court authorize CSIS to obtain BII in respect of communications accounts corresponding to telephone numbers or electronic identifiers that may in the future come to its attention in the course of its investigations, where CSIS has not described and established their specific nexus to those investigations?

ii. Can the Court authorize CSIS to obtain BII in respect of communications accounts identified pursuant to its review of specifically defined information obtained in relation to [redacted] named individuals and [redacted] additional individuals who have been identified [redacted]

iii. Can the Court authorize an employee of CSIS to obtain BII in respect of a communications account that corresponds to a telephone number or an electronic identifier, where a "Chief" within CSIS determines that the account was identified during its investigation, and that the BII would assist CSIS in its investigation?

[43] In both [redacted] and [redacted] the Attorney General raised an additional issue, namely, the threshold issue of whether a warrant is required to obtain BII from a CSP. However, in each proceeding, the Attorney General conceded that a warrant is required to obtain BII from a CSP, because it may engage privacy rights that are protected by section 8 of the *Charter*. This is because "[redacted] information can be revealed to [CSIS] when BII is obtained from CSPs." Indeed, this was demonstrated by a number of examples included in the Attorney General's written submissions.

[44] The *Amici* agreed. They maintained that, in view of the fact that CSIS may well be able to use BII [redacted] to link previously anonymous [redacted] activity to a named individual, such activity by CSIS would normally require a warrant. I agree.

[45] Given the Attorney General's acknowledgement that a warrant is required to access BII from a CSP, it is unnecessary to address this issue in detail. I will simply note that the linking of previously anonymous [redacted] activity to an individual's identity "engages a high level of informational privacy" (*R v Spencer*, 2014 SCC 43, at para 51 [*Spencer*]). As such, obtaining the information to make such a link, [redacted] would

constitute a "search" that is more invasive than the minimally intrusive warrantless searches that are authorized by section 12 of the Act.

[46] The same is true with respect to telephone numbers, which can assist CSIS to obtain valuable personal information about a person. This was corroborated by one of the examples provided by Mr. [redacted] in his affidavit.

[47] I will simply add that the Attorney General's position that a warrant is required to obtain BII is consistent with the position that she took in [redacted] where she stated on multiple occasions that a warrant would be required to obtain subscriber information pertaining to any identifiers [redacted]

V. Analysis

A. *Applicable legal principles*

[48] Section 8 of the Charter provides that "[e]veryone has the right to be secure against unreasonable search or seizure."

[49] It follows that section 8 of the *Charter* does not afford protection against all searches, only against *unreasonable* ones (*R v Gomboc*, 2010 SCC 55, at para 20 [*Gomboc*]).

[50] In assessing whether a search is "unreasonable," courts must adopt "a purposive approach that emphasizes the protection of privacy as a prerequisite to individual security, self-fulfilment

and autonomy as well as to the maintenance of a thriving democratic society" (*Spencer*, above, at para 15).

[51] Broadly speaking, a determination of whether a search is unreasonable requires a balancing assessment of "whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals" (*Hunter et al v Southam Inc*, [1984] 2 SCR 145, at 159–160 [*Hunter*]).

[52] Given that the underlying purpose of section 8 is to protect individuals from unjustified state intrusions upon their privacy, prior authorization of those intrusions is presumptively required. Such authorization must be given by an entirely neutral and impartial arbiter who is capable of acting judicially in balancing the interests of the state against those of the individual (*Spencer*, above, at para 68; *Goodwin v BC (Superintendent of Motor Vehicles)*, 2015 SCC 46, at para 56 [*Goodwin*]; *Hunter*, above, at 160-162).

[53] In addition, the neutral arbiter must be satisfied that the person seeking the authorization has reasonable grounds, established under oath, to believe that the relevant statutory or other conditions to be met before the search power may be exercised, have in fact been met (*Hunter*, above, at 166-168).

[54] In deciding whether to issue a warrant, the neutral arbiter must have sufficient flexibility to consider all of the circumstances that may be relevant to the exercise of discretion to issue the

warrant, and to impose any conditions that may be considered necessary (*Baron v Canada*, [1993] 1 SCR 416, at paras 437, 439, 440 [*Baron*]).

B. *Can the Court authorize CSIS to obtain BII in respect of communications accounts corresponding to telephone numbers or electronic identifiers that may in the future come to its attention in the course of its investigations, where CSIS has not described and established their specific nexus to those investigations?*

(1) General

[55] In her written and oral submissions, the Attorney General characterized this issue as being whether the Act authorizes a judge of this Court to issue warrants against "threat-related activities."

[56] In support of her position that the Act is sufficiently flexible to allow for the issuance of warrants in respect of *activities*, the Attorney General notes that section 12 of the Act empowers CSIS to investigate activities, and that the definition of "threats to the security of Canada" that is set forth in section 2 of the Act also refers to *activities*, without any reference to the *persons* who would be conducting those activities. The Attorney General further notes that paragraph 21(2)(d) requires a warrant application to be accompanied by an affidavit that addresses various issues, including "the identity of the person, <u>if known</u>, whose communication is proposed to be intercepted or who has possession of the information, record, document or other thing proposed to be obtained" (emphasis added).

[57] The Attorney General submits that it may be inferred from all of the foregoing that warrants issued pursuant to section 21 of the Act can be obtained to investigate identified threat-

related activities. She maintains that this is so even where the warrant does not name any individuals or describe the specific nexus between CSIS's investigation and the individuals whose privacy interests would be intruded upon.

[58] I disagree. With respect, that position confuses the activities that CSIS is authorized to investigate under section 12 of the Act, with the privacy interests that might be engaged by a warrant issued under section 21 in connection with an investigation. Privacy interests are not held by activities or threats, such as those posed by [redacted] or "Islamist terrorism," or in respect of an event that might be the focus of an investigation, such as the Vancouver Olympics or the G7 meeting that took place in Toronto.

[59] Privacy interests are held by individuals and corporations, whether they be subjects of investigation, persons whose connection to an investigation may remain to be ascertained, or persons who might, on reasonable grounds, be believed to have information that is likely to assist an investigation. In my view, the words "the identity of the person, if known" (emphasis added) in paragraph 21(2)(d) simply reflects the practical reality that CSIS may not know, at the time it applies for a warrant, the identity of an ascertainable person whose communication is proposed to be intercepted, or who has possession of the information, record, document or other thing proposed to be obtained under the warrant, as contemplated by that provision.

[60] Accordingly, the more relevant question that arises in these proceedings is whether CSIS can be prospectively authorized to obtain BII in relation to communications accounts that may in the future come to its attention in the course of its investigations, where CSIS has not yet

described and established their specific nexus with those investigations. In my view, the answer is "no, except in exceptional circumstances that have not been demonstrated to exist in this case."

[61] This is because persons who are responsible for authorizing the use of intrusive powers are required to consider the impact of such intrusion on the specific "subject of the search" (*Hunter*, above, at 157; *Spencer*, above, at para 36 (emphasis added)). In other words, an assessment must be made of the context of each "particular situation," and its impact on "the individual." As the *Amici* underscored, the balancing analysis to be conducted is between the interests of the state and the interests of the specific individual whose privacy interests are at issue (*Hunter*, above, at 159-160, 161-162, 167; *Baron*, above, at 435-436, 437; *R v Rodgers*, 2006 SCC 15, at para 27 (emphasis added)).

[62] Where a "class of persons" whose privacy interests may be encroached upon can be described in a manner that enables the Court to clearly understand the nexus between those persons and the threat-related activities that are the focus of a CSIS investigation, the balancing analysis described above can comfortably be conducted in respect of those persons. In my view, this is contemplated by the references to "class of persons" in paragraphs 21(2)(e) and 21(4)(c) of the Act.

[63] The need to consider the interests of the specific individual or class of individuals whose privacy interests are engaged is reinforced by three additional requirements that have been established by jurisprudence under section 8 of the *Charter*. The first is the requirement to assess

the individual's subjective expectation of privacy, when considering whether there is a reasonable expectation of privacy (*Spencer*, above, at para 18). The second is the requirement that CSIS's powers to investigate activities that pose threats to the security of Canada must be "strictly controlled" (*Charkaoui v Canada*, 2008 SCC 38, at para 22 [*Charkaoui*], quoting the *Report of the Special Senate Committee on the Canadian Security Intelligence Service, Delicate Balance: A Security Intelligence Service in a Democratic Society*, November 3, 1983, at para 25; see also *Baron*, above, at 436-437). The third is the requirement to consider "the totality of the circumstances" (*Spencer*, above, at para 18). In my view, this implies that the interests of the specific person(s) whose privacy interests are at stake must be taken into account. It is difficult to imagine how the totality of the circumstances would not involve an assessment of the privacy interests of the very individual(s) whose interests would be engaged if CSIS were to obtain BII from a CSP.

[64] Notwithstanding the foregoing, it is not necessary for warrants that authorize CSIS to obtain BII to associate the communications accounts in question with named individuals. It is often precisely because CSIS does not know the name associated with a telephone number, [or an electronic identifier] etc. that it needs to be able to obtain BII in respect of the corresponding communications account from a CSP.

[65] Even though CSIS may not know an individual's name, it may know sufficient information about the individual to provide the Court with reasonable grounds to believe that obtaining the BII of a particular communications accounts is required to advance its investigation, as contemplated by paragraph 21(2)(a) of the Act. This may

be because the individual behind a telephone number or electronic identifier appears to be engaged in activities that pose a threat to the security of Canada, or because he or she appears to be in a position to provide information that will assist CSIS to advance its investigation into those activities. I accept Mr. [redacted] testimony that obtaining BII, and thereby learning who is behind [redacted] identifiers [redacted] can assist CSIS to advance an investigation.

[66] In such situations, it will suffice if CSIS can provide sufficient evidence about a telephone number or one of the types of other identifiers mentioned above to establish reasonable grounds to believe that CSIS requires the BII of the account corresponding to that number or identifier, to advance its investigation. In my experience, those grounds can often be established by providing the Court with a brief description of the context in which CSIS obtained the telephone number or other identifier in respect of which BII is sought. It is that specific context that can provide the Court with the nexus between the unidentified individual whose privacy rights will be engaged by the BII power, and CSIS's investigation.

[67] Where CSIS is not in possession of the telephone number or other identifier at the time of a warrant application for authorization to obtain BII information, it will remain open to CSIS to describe the telephone number or identifier in a way that enables the Court to satisfy itself of the matters referred to in paragraphs 21(2)(a) and (b) of the Act. With respect to the reasonable grounds to believe referred to in paragraph 21(2)(a), it may suffice to provide the Court with an understanding of the nexus between CSIS's investigation and the specific individual(s) whose privacy interests would be intruded upon. For example, it may suffice to describe a telephone

number in terms of a future communication by a subject of investigation. If there were reasonable grounds to believe that the subject of investigation may be engaged in activities that pose a threat to the security of Canada, there would be reasonable grounds to believe that the BII associated with the telephone numbers at each end of a future call placed or received by that individual is required to assist CSIS to advance its investigation of the threat-related activities of that person. Stated differently, this information would provide the Court with the reasonable basis contemplated by section 8 of the *Charter* on which to authorize CSIS to obtain the BII pertaining to the accounts of both the subject of investigation, and the yet-to-be identified third parties with whom he or she may communicate.

[68] For the same reason, it may suffice for CSIS to describe a BII authorization that it may wish to seek, by reference to a [landline or electronic account] account that CSIS may in the future discover has been used by a subject of investigation. The same would apply with respect to [landline or electronic account] accounts that CSIS may in the future discover are used by individuals [redacted] Of course, CSIS would have to establish at the time it seeks the BII authorization in question that there are reasonable grounds to believe that persons [redacted] may have been associated with the threat-related activities in question.

[69] In my view, the foregoing examples would meet the requirements of both section 21 of the Act and section 8 of the *Charter*. They strike an appropriate balance between the public interest in affording CSIS with a reasonable degree of flexibility to fulfill its statutory mandate,

and the privacy interests of yet-to-be identified individuals whose BII would be obtained under a warrant. Among other things, those examples help to respond to the practical difficulty associated with threat-related activities in respect of future events (*Atwal v Canada*, [1988] 1 FC 107, 127 [*Atwal*]).

(2) The BII Warrant and the first type of proposed amendments to the warrants issued in [redacted]

[70] With the foregoing in mind, it should be readily apparent that the appropriate balance is not met with the BII Warrant that CSIS has sought in [redacted] or with the first type of amendments that have been proposed to three of the warrants that were issued in [redacted]

[71] This is because the requested authorizations would permit CSIS to obtain BII in respect of any communications accounts that CSIS may identify over the course of very broadly defined investigations into threats to the security of Canada posed by Islamist terrorism and certain activities of [redacted] where CSIS simply determines that BII will assist it in its investigation. Among other things, CSIS has not provided the Court with any understanding whatsoever of the specific nexus between (i) the as-yet-to be discovered telephone numbers and electronic identifiers in respect of which BII would be sought, and (ii) CSIS's investigations. The loosely defined "nexus" is simply too broad and nebulous (*R v Chehil*, 2013 SCC 49, at paras 36 and 51). And it does not provide sufficient information for the Court to be satisfied that such BII information is required to enable CSIS to investigate the threat to the security of Canada posed by Islamist terrorism, as contemplated by paragraph 21(2)(a) of the Act.

[72] As I have noted earlier, CSIS has described the threat to the security of Canada in [redacted] in terms of "activities in paragraph (c) of the definition of 'threats to the security of Canada' found in section 2 of the Act that are [redacted]

[73] The language of the proposed BII Warrant does not enable the Court to know with which of the [redacted] identified [redacted] groups a communications account would be associated. Indeed, it does not even enable the Court to know the [redacted] to which the telephone number or identifier would pertain. In my view, this does not permit the Court to have a sufficient sense of the nexus between the identified threat-related activities of Islamist terrorism and the individual whose privacy rights would be encroached upon to be considered "reasonable" within the meaning of section 8 of the *Charter*.

[74] This problem, which is fatal in and of itself, is exacerbated by the fact that one of the clauses in the BII Warrant that I initially assumed would limit, at least to some extent, the scope of the warrant, will not in fact have that effect. Specifically, I had assumed that the words "where a Chief determines that […] the identity of the subscriber to the account will assist in the investigation of Islamist terrorism," would place some important limit on the scope of the warrant. However, Mr. [redacted] testified that obtaining BII will <u>always</u> assist CSIS's investigation, even if it merely confirms that the individual who is identified through the BII is of no value to the investigation. Mr. [redacted] explained that even just eliminating a person from further consideration will invariably assist an investigation. The logical extension of that argument is

that obtaining the BII corresponding to any and all accounts that are merely identified in the course of an investigation will always assist in that investigation**.**

[75] I will pause here to observe that one of the consequences of a determination that the BII of any account will assist in CSIS's investigation is that CSIS would retain collected information indefinitely. Another consequence is that such information may well be shared with a foreign intelligence agency.

[76] The same problems exist with the first of the two types of BII authorizations that CSIS requested be added to three of the warrants that were issued in the first phase of [redacted] I recognize that the threat-related activities in [redacted] are more narrowly defined than they are in [redacted] as they are confined to activities of [redacted] that fall within paragraphs (a) and (b) of the definition of "threats to the security of Canada" set forth in section 2 of the Act. Nevertheless, to the extent that the language of the first group of authorizations sought in the requested warrant amendments in [redacted] is virtually identical to the language of the BII Warrant being sought in [redacted] it suffers from the same fatal flaw of overbreadth. This is because the Court has no understanding whatsoever of the specific nexus between the as-yet-to be discovered telephone numbers or electronic identifiers, and CSIS's investigation.

[77] In passing, I will pause to recognize that in exceptional circumstances, CSIS may require BII or similar information in a shorter timeframe than may be needed to obtain a warrant or an amendment to an existing warrant. One such circumstance was the focus of an [redacted]

Warrant that was sought and granted in [redacted] There, Justice Noël recognized that CSIS needed to be able to investigate threat-related [redacted] Accordingly, he authorized CSIS to obtain subscriber information [redacted] during its investigation of the threat to the security of Canada in question, where a Regional Director General or his designated had reasonable grounds to believe that such information might assist in that investigation. [redacted] However, CSIS was then subject to a condition that required it to bring a further application to the Court, without delay, to execute the warranted powers in respect of any [redacted] all as defined in the warrant.

[78] In my view, no exceptional situation of this nature, or any other nature, has been identified in these proceedings.

C. *Can the Court authorize CSIS to obtain BII in respect of communications accounts identified pursuant to its review of specifically defined information obtained in relation to [redacted] individuals and [redacted] additional individuals who have been identified* [redacted]

[79] This issue is raised solely in respect of the second type of BII authorization that CSIS has requested be added to three of the warrants in [redacted] This authorization would enable CSIS to obtain BII in respect of communications accounts identified pursuant to its review of specifically defined information obtained in relation to [redacted] named individuals and [redacted] additional individuals who have been identified [redacted]

[80] In my view, this authorization does not suffer from the defects described in the preceding section above. It is perhaps for that reason that it was not the subject of significant submissions by the Attorney General or the *Amici* in these applications. Accordingly, I will only deal with this type of authorization briefly.

[81] In contrast to the first type of authorization sought in [redacted] and to the BII Warrant sought in [redacted] the Court has been provided with the information that it requires to grant the authorization. That is to say, it has been provided with sufficient information to have reasonable grounds to believe that the BII of the specific individuals whose privacy rights would be encroached upon is required to assist CSIS to advance its investigation into [redacted] threat-related activities.

[82] Specifically, paragraph 10(a) of the [redacted] would authorize the Director of CSIS and any employee of CSIS acting under his authority to obtain BII in respect of any third party account with a CSP that CSIS may identify during its review of:

i. [redacted] [the Identified Individuals];

ii. [redacted]

iii. [redacted]

iv. [redacted]

[83] CSIS seeks to include essentially the same authorization in paragraph 2(a) of the [redacted] and in paragraph 5(a) of the [redacted]

[84] The information described at paragraph 82 above all relates directly to [redacted] individuals who are subjects of investigation. There are reasonable grounds to believe that those individuals may be engaged in activities that constitute threats to the security of Canada. Based on those facts, I am satisfied that CSIS has established reasonable grounds to believe that BII in respect of telephone numbers or electronic identifiers that it may identify, after reviewing the information described at paragraph 82 above, is required to enable CSIS to advance its investigation into the threat-related activities [redacted]

[85] I will simply add in passing that I am satisfied that the other preconditions to obtaining a warrant, as set forth in paragraph 21(2)(b) of the Act, have been met.

[86] In summary, I will grant the second group of requested amendments to three of the warrants that were previously issued by Justice Noël in [redacted] to enable CSIS to obtain BII

in respect of communications accounts of third parties that may be identified pursuant to its review of the information of the Identified Individuals that is described at paragraph 82 above.

[87] Nevertheless, I have a concern regarding the potentially large number of third parties whose BII may be obtained by CSIS, as a result of the execution of this BII authorization in respect of the [redacted] Individuals who are targets [redacted] Those [redacted] respectively. Given the nature of [redacted] it is reasonably foreseeable that a potentially large number of members of the public who communicate with those individuals for entirely legitimate purposes will come within the scope of the BII authorization. And once subject to that authorization, their BII may be obtained by CSIS and retained indefinitely. Accordingly, it will be necessary to develop some conditions to address these issues.

D. *Can the Court authorize an employee of CSIS to obtain BII of a communications account that corresponds to a telephone number or an electronic identifier, where a "Chief" within CSIS determines that the account was identified during its investigation, and that the BII would assist CSIS in its investigation?*

[88] The Attorney General submits that a judge of this Court has the required discretion to allow a designated employee within CSIS to determine whether prescribed circumstances have been met for CSIS to request and obtain BII from a CSP. In this regard, the Attorney General maintains that discretion may rest with those responsible for the execution of a warrant, because such discretion will frequently be necessary. For example, she notes that general warrants issued under the *Criminal Code*, RSC, 1985, c C-46, often allow police a degree of discretion that is reasonably necessary to carry out a search (*R v Poirier*, 2016 ONCA 582, at paras 34 and 49),

to search things that are not identified in the warrant (*R v Noseworthy* (1997), 33 OR (3d) 641), or to search during a timeframe that is not specified in the warrant (*R v Telus Communications Co.*, 2013 3 SCC 16, [2013] 2 SCR 3 at para 69).

[89] The Attorney General asserts that the discretion being sought is appropriate because of several safeguards that have been put in place to ensure that there is only a minimal impact on any privacy rights that may be engaged as a result of CSIS obtaining access to BII, and to ensure compliance with what the Court will be authorizing. Those safeguards are as follows:

i. Before making a request for BII from a CSP, CSIS will first try to confirm the identity of the subscriber in question by other means.

ii. Each request for BII from a CSP [redacted]

iii. Before a Chief may approve a request for BII, he must be satisfied that the circumstances specified in the warrant exist, namely that (i) the telephone number or [electronic identifier] was identified in the course of the investigation in question, and (ii) obtaining the identity of the subscriber will assist in that investigation.

iv. The BII authorization provides that, when CSIS [redacted]

v. [redacted]

vi. CSIS will be required to destroy any information provided by a CSP that does not fall within the strict definition of BII.

[90] The *Amici* acknowledge that agents of the state such as CSIS may be accorded a certain degree of discretion with respect to the *manner* in which a warrant is executed, including the discretion to do what is reasonably necessary to execute the warranted powers, and some temporal flexibility. However, they maintain that the BII Warrant and the first type of proposed amendments to the warrants that were issued in [redacted] go far beyond the discretion that may be granted to CSIS with respect to the *execution* of the proposed warranted powers.

[91] I agree. In my view, those proposed authorizations would impermissibly delegate to a person holding the position of "Chief" within CSIS a function that must be performed by a designated judge of this Court (*Canadian Security Intelligence Service Act (Re)*, [1998] 1 FC 420, at para 17 [*CSIS Act (Re)*]). That function is the determination of which specific communications accounts will be the subject of requests to CSPs for BII. In the exercise of that function, persons holding the position of "Chief" within CSIS would, in essence, make

the determination of whether the grounds that must be established before a specific individual's privacy interests can be intruded upon, have been met.

[92] Only a designated judge can make such determinations in respect of the exercise of powers by CSIS that are more than minimally intrusive in nature. In conceding that a warrant is required to obtain the proposed authorizations, the Attorney General has also effectively conceded that those authorizations would be more than minimally intrusive in nature.

[93] An authorization for CSIS to engage in what amounts to a search that is more than minimally invasive in nature must be given by an entirely neutral and impartial arbiter who is capable of acting judicially in balancing the interests of the state against those of the individual whose privacy rights would be encroached upon (*Spencer*, above, at para 68; *Goodwin*, above, at para 56; *Hunter*, above, at 160-162; *R v Thompson*, [1990] 2 SCR 1111, at 1134*; R v Grabowski*, [1985] 2 SCR 434, at 445-446).

[94] An individual holding the position of Chief within CSIS is not capable of acting judicially in this regard, because such individuals cannot neutrally and impartially conduct that balancing exercise. As employees of CSIS, they are not neutral or independent in the sense required by the jurisprudence. In other words, the nature of their investigative functions "ill-accords with the neutrality and detachment necessary to assess whether the evidence reveals that the point has been reached where the interests of the individual must constitutionally give way to those of the state" (*Hunter*, above, at 164; *R v Généreux*, [1992] 1 SCR 259, at 311-312).

[95] This is borne out by the testimony provided by Mr. [redacted] regarding the likely incentives of an individual holding the position of Chief within CSIS. For example, at one point during the hearing, Mr. [redacted] stated:

> I think the Chief's incentive is the same as everybody else's incentive. It's to determine whether or not there is a threat activity going on, to determine whether or not there is a threat to national security, and if so, to be in a position to investigate it and thereby be able to inform the government.

[96] In response to further questioning from the Court on this point, he stated:

> To me the calculus on this one is very easy. The risk of not pursuing means I have a potential threat that I know nothing about, and I'm not willing to live with that.

[97] Elsewhere, he observed:

> […] I am not sure that the risk that the Chief would be assessing would be the risk of doing it but perhaps the risk of not doing it.
>
> If we had a situation where there is a piece of information that is missing from the puzzle and I believe as the Chief, if I am signing this, that to get that piece of information will advance my investigation and allow me to have a better overview of the situation, then the risk of not doing that is I can't do my job. I can't provide that value added advice to the Government of Canada. I can't tell them what the threat is.

[98] In my view, it is readily apparent from the foregoing passages of Mr. [redacted] testimony that a Chief within CSIS would have a bias towards authorizing the obtaining of BII from a CSP any time that he thought that this would advance CSIS's investigation. And as discussed at paragraph 74 above, Mr. [redacted] also testified that obtaining BII would *always* advance CSIS's investigation, even where it simply assists CSIS to determine that the individual behind a

telephone number or electronic identifier is not involved in threat-related activities, and therefore cannot provide information that will assist CSIS to advance its investigation.

[99] In summary, this Court cannot authorize an employee within CSIS to obtain BII corresponding to a telephone or an electronic identifier, where a "Chief" within CSIS determines that the account was identified during its investigation, and that the BII would assist CSIS in its investigation. Determinations as to which specific communications accounts may be the subject of requests to CSPs for BII must be made by a designated judge of this Court. Allowing such determinations to be made by a Chief within CSIS would constitute an impermissible delegation of the Court's responsibility to determine whether the grounds to be met before an individual's privacy interests can be intruded upon, have been met. Moreover, Chiefs within CSIS would not have the required degree of neutrality and impartiality to perform this important function.

[100] In my view, all of the foregoing is rendered even more troublesome by (i) the very broad definition of Islamist terrorism that CSIS has adopted, (ii) the fact that CSIS would indefinitely retain all of the BII that it seeks to obtain under the requested authorizations, and (iii) the fact that there would be no limit whatsoever on CSIS's ability to share that information with foreign intelligence agencies.

[101] The defects identified above do not exist with respect to the second type of authorization that CSIS has sought in [redacted] This is because the Court is able to perform, *in advance*, the required balancing assessment in respect of the privacy rights of the ascertainable, but yet-to-be identified third parties behind those telephone numbers and electronic identifiers, and the

interests of the state. As in *Thompson*, above, those yet-to-be identified third parties can be ascertained and circumscribed by reference to their communications with known subjects of investigation who have been identified in the warrant (*Thompson*, above 1134-1135).

[102] In brief, once the Court is satisfied that there are reasonable grounds to believe that the Identified Individuals are engaged in activities that may pose a threat to the security of Canada, it has a specific basis upon which to be satisfied on that basis alone that there are reasonable grounds to believe that third parties, with whom the Identified Individuals are communicating, may have information that will assist CSIS to advance its investigation, and that, therefore, CSIS requires the BII in question in order to advance its investigation.

VI. Conclusion

[103] For the reasons set forth in Parts V.B and D. above, the Court cannot provide the broad authorization that CSIS has sought in the BII Warrant and in the first type of proposed amendments to three of the warrants that were issued in the first phase of [redacted]

[104] This is so for two principal reasons. First, CSIS has not established and described the specific and required nexus between (i) the future telephone numbers and electronic identifiers that it may identify, and in respect of which it would like to be authorized prospectively to obtain BII, and (ii) its investigations into Islamist terrorism, or the threat-related activities [redacted] respectively. The loosely defined "nexus" that CSIS has described is simply too broad and nebulous. Moreover, CSIS has not provided sufficient information for the Court to be satisfied

that BII is required to enable it to investigate the threats to the security of Canada posed by Islamist terrorism and [redacted] as contemplated by paragraph 21(2)(a) of the Act.

[105] Second, that proposed authorization would impermissibly delegate to a person holding the position of "Chief" within CSIS a function that must be performed by a designated judge of this Court. That function is the determination of whether the grounds that must be established before a specific individual's privacy interests can be intruded upon, have been met. Quite apart from the fact that this is a function that must be performed by a designated judge of this Court, a Chief within CSIS is not capable of making the required determination in a neutral and unbiased manner, as required by section 8 of the *Charter*.

[106] However, for the reasons set forth in Part V.C above, the Court is able to authorize the second group of amendments that CSIS has proposed be made to the warrants that were granted in [redacted] This is because CSIS has established reasonable grounds to believe that BII information in respect of telephone numbers or electronic identifiers that it may identify after reviewing the information described at paragraph 82 above, is required to enable CSIS to advance its investigation. That information all relates directly to [redacted] Identified Individuals who are subjects of investigation.

[107] Given the conclusion that I have reached with respect to the BII Warrant and the first group of amendments that CSIS has proposed in [redacted] it will be necessary for CSIS to seek an authorization from the Court each time it identifies additional telephone numbers or electronic identifiers in respect of which it wishes to obtain BII from a CSP. At that time, CSIS will have to

establish a sufficient nexus between the telephone number or other identifier in question and its investigation to satisfy the Court that there are reasonable grounds to believe that CSIS requires the BII of the corresponding communications account to advance its investigation.

[108] This is subject to the *proviso* that CSIS need not return to the Court when it has already obtained an advance authorization to obtain the BII of communications accounts corresponding to the telephone numbers or electronic identifiers of ascertainable, but yet-to-be identified individuals, such as those described in paragraphs 65-69 and 101-102 above.

[109] I recognize that the conclusion I have reached will likely impose an additional burden on CSIS. I also recognize that this may give rise to additional costs and delays associated with obtaining BII authorizations in relation to telephone numbers or electronic identifiers that may come to CSIS's attention during the course of its investigations into Islamist terrorism and the threat-related activities [redacted] and which are not linked with a target that is the subject of a warrant. Given the adverse implications that the potential delays, in particular, may have for CSIS's ability to investigate threat-related activities, the Court will remain open to considering alternate approaches that are *Charter* compliant.

[110] In this regard, I note that CSIS already has an internal process in place that requires those who wish to seek warrant powers to explain why they require BII in respect of a telephone number or an electronic identifier that has been identified in the course of an investigation. Those explanations are provided in [redacted] forms, a number of examples of which were provided to the Court in the course of these applications. In my view,

many of the examples of [redacted] forms provided to the Court contain sufficient information to provide the Court with reasonable grounds to believe that the BII in question was required to enable CSIS to investigate the threat-related activities of Islamist terrorism and [redacted]

[111] I find it difficult to understand why it would require substantial time and effort to provide the Court with essentially the same information that has already been prepared by CSIS internally. If such information were simply provided by way of a supplementary affidavit, together with a proposed amendment to an existing warrant, the time and effort that would be required on CSIS's part may not be unduly onerous at all.

JUDGMENT in [redacted]

THIS COURT'S JUDGMENT is that this application is dismissed.

JUDGMENT in [redacted]

THIS COURT'S JUDGMENT is that this application is dismissed in part. Specifically:

1. For the reasons provided in Parts V.B. and D. of the attached Judgment and Reasons, the following amendments that the Attorney General has sought to three of the warrants that were issued by Justice Noël during the first phase of this application will be not be granted:
    i. [redacted] new paragraph 10(b);
    ii. [redacted] new paragraph 5(b);
    iii. [redacted] new paragraph 2(b));
2. For the Reasons provided in Part V.C. of the attached Judgment and Reasons, the other amendments that the Attorney General has sought to the aforementioned warrants will be granted.

The present Judgment and Reasons shall, within seven (7) days of receipt, be reviewed jointly by the *amici curiae* and the Attorney General with a view to making a joint recommendation to the Court regarding redactions to the version of the Judgment and Reasons that will be made public. The Attorney General and the *Amici* must be guided by the open Court principle in their consultation and determination. Any contentious issues shall be drawn to my

attention or to the attention of another designated judge, if I am unable to exercise my judicial function.

"Paul S. Crampton"
Chief Justice

APPENDIX I

CANADIAN SECURITY INTELLIGENCE SERVICE ACT, RSC, 1985, C C-23

Definitions

2 In this Act,

threats to the security of Canada means

(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,

(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,

(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 Canada or a foreign state, and

(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,

LOI SUR LE SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ, LRC (1985), CH C-23

Définitions

2 Les définitions qui suivent s'appliquent à la présente loi.

menaces envers la sécurité du Canada

Constituent des menaces envers la sécurité du Canada les activités suivantes :

a) l'espionnage ou le sabotage visant le Canada ou préjudiciables à ses intérêts, ainsi que les activités tendant à favoriser ce genre

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) les activités qui touchent le Canada ou s'y déroulent et visent à favoriser l'usage de la violence grave ou de menaces de violence contre des personnes ou des biens dans le but d'atteindre un objectif politique, religieux ou idéologique au Canada ou dans un État étranger;

d) les activités qui, par des actions cachées et illicites, visent à saper le régime de gouvernement constitutionnellement établi au Canada ou dont le but immédiat ou ultime est sa destruction ou son renversement, par la violence.

but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (a) to (d). (menaces envers la sécurité du Canada)

La présente définition ne vise toutefois pas les activités licites de défense d'une cause, de protestation ou de manifestation d'un désaccord qui n'ont aucun lien avec les activités mentionnées aux alinéas a) à d). (threats to the security of Canada)

Duties and Functions of Service

Collection, analysis and retention

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.

No territorial limit

(2) For greater certainty, the Service may perform its duties and functions under subsection (1) within or outside Canada.

Fonctions du Service

Informations et renseignements

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.

Aucune limite territoriale

(2) Il est entendu que le Service peut exercer les fonctions que le paragraphe (1) lui confère même à l'extérieur du Canada.

Judicial Control

Application for warrant

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.

Contrôle judiciaire

Demande de mandat

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

Matters to be specified in application for warrant

(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,

(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;

(b) that other investigative procedures have been tried and have failed or why it appears that they are unlikely to succeed, that the urgency of the matter is such that it would be impractical to carry out the investigation using only other investigative procedures or that without a warrant under this section it is likely that information of importance with respect to the threat to the security of Canada or the performance of the duties and functions under section 16 referred to in paragraph (a) would not be obtained;

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

(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;

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

Contenu de la demande

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

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) le fait que d'autres méthodes d'enquête ont été essayées en vain, ou la raison pour laquelle elles semblent avoir peu de chances de succès, le fait que l'urgence de l'affaire est telle qu'il serait très difficile de mener l'enquête sans mandat ou le fait que, sans mandat, il est probable que des informations importantes concernant les menaces ou les fonctions visées au paragraphe (1) ne pourraient être acquises;

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

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

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

g) the period, not exceeding sixty days or one year, as the case may be, for which the warrant is requested to be in force that is applicable by virtue of subsection (5); and

g) la durée de validité applicable en vertu du paragraphe (5), de soixante jours ou d'un an au maximum, selon le cas, demandée pour le mandat;

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

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

Issuance of warrant

Délivrance du mandat

(3) Notwithstanding any other law but subject to the Statistics Act, where the judge to whom an application under subsection (1) is made is satisfied of the matters referred to in paragraphs (2)(a) and (b) set out in the affidavit accompanying the application, the judge may issue a warrant authorizing the persons to whom it is directed to intercept any communication or obtain any information, record, document or thing and, for that purpose,

(3) Par dérogation à toute autre règle de droit mais sous réserve de la Loi sur la statistique, le juge à qui est présentée la demande visée au paragraphe (1) peut décerner le mandat s'il est convaincu de l'existence des faits mentionnés aux alinéas (2)a) et b) et dans l'affidavit qui accompagne la demande; le mandat autorise ses destinataires à intercepter des communications ou à acquérir des informations, documents ou objets. À cette fin, il peut autoriser aussi, de leur part :

(a) to enter any place or open or obtain access 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.

Activities outside Canada

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

Activités à l'extérieur du Canada

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

Matters to be specified in warrant

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

Contenu du mandat

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

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

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

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

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

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

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

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

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

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

e) la durée de validité du mandat;

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

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

Maximum duration of warrant

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

(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

(b) one year in any other case.

Durée maximale

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

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) d'un an, dans tout autre cas.

FEDERAL COURT

SOLICITORS OF RECORD

DOCKETS:	[redacted] AND [redacted]
STYLE OF CAUSE:	IN THE MATTER OF AN APPLICATION BY [redacted] FOR WARRANTS PURSUANT TO SECTIONS 12 AND 21 OF THE *CANADIAN SECURITY INTELLIGENCE SERVICE ACT*, RSC 1985, c C-23 AND IN THE MATTER OF [redacted] THREAT-RELATED ACTIVITIES AND IN THE MATTER OF AN APPLICATION BY [redacted] FOR WARRANTS PURSUANT TO SECTIONS 12 AND 21 OF THE *CANADIAN SECURITY INTELLIGENCE SERVICE ACT*, c C-23 AND IN THE MATTER OF ISLAMIST TERRORISM
PLACE OF HEARING:	OTTAWA, ONTARIO
DATE OF HEARING:	MAY 25, 26 AND JUNE 23, 2017
JUDGMENT AND REASONS:	CRAMPTON C.J.
DATED:	SEPTEMBER 27, 2017

APPEARANCES:

Ms. Karla Unger Mr. Gordon Kirk Ms. Nathalie Benoit	DEPARTMENT OF JUSTICE NATIONAL SECURITY LITIGATION AND ADVISORY GROUP
Mr. Gordon Cameron Mr. Owen Rees	*AMICUS CURIAE*

SOLICITORS OF RECORD:

Natalie G. Drouin
Deputy Attorney General of
Canada
Ottawa, Ontario

DEPARTMENT OF JUSTICE
NATIONAL SECURITY LITIGATION
AND ADVISORY GROUP

Blakes Cassels & Graydon LLP
Ottawa, Ontario

BARRISTERS AND SOLICITORS

Conway Baxter Wilson LLP
Ottawa, Ontario