Federal Court Cour fédérale

TOP SECRET

Date: 20180830

Docket: [redacted]

CONF-2-18

Citation Number: 2018 FC 874

Ottawa, Ontario, August 30, 2018

PRESENT: THE CHIEF JUSTICE

BETWEEN:

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

and

IN THE MATTER OF ISLAMIST TERRORISM

REASONS

CRAMPTON C.J.

I. Introduction

[1] This Court is committed to increasing the transparency of its decisions in private proceedings under the *Canadian Security Intelligence Service Act*, R.S.C. 1985, C.c-23 [the **Act**]. In furtherance of that objective, I have described below a series of developments that

have occurred with respect to a particular type of warrant power, subsequent to my decision in *X (Re)*, 2017 FC 1048 [***X (Re)*****].**

[2] In *X (Re)*, I rejected an application for that warrant power, due to deficiencies in the application. I ultimately granted an application for essentially the same warrant power in the present proceeding after satisfying myself that those deficiencies, and others that were identified in the intervening applications discussed below, had been overcome. The paragraphs below explain why this is so.

[3] The warrant power in question concerns the ability of the Canadian Security Intelligence Service [**CSIS**] to obtain basic identifying information [**BII**] from communications service providers [**CSPs**]. In the past, that information has pertained to communications accounts of individuals whose telephone number, [redacted] or other electronic identifiers might, at a future date, come to CSIS's attention in the course of its investigations. Those investigations have concerned identified activities that CSIS has established constitute threats to the security of Canada.

[4] BII consists of the name and address of a subscriber to a communications account, [redacted]

[redacted]

[5] In *X (Re)*, above, I concluded that the Court cannot 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. In my view, a request to obtain such a power in those circumstances does not meet the basic requirements for authorizing intrusive activity by the state. I summarized the basis for this view as follows:

> [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* [the Act], in respect of such person or class of persons.

[6] Given that the Court had not been provided with such an understanding of the nexus described above in respect of the broad BII warrant power that CSIS had sought in [redacted] separate applications in *Re (X)*, I refused CSIS's requests for those powers. In brief, for the reasons set forth in the passage quoted immediately above, those requests were not compliant with 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***], which guarantees the right to be secure against unreasonable search or seizure: *X (Re)*, above, at paras 60-74.

[7] In reaching my decision in *X (Re)*, I recognized that the position set forth above would impose a potentially significant additional burden on CSIS. In this regard I observed as follows:

> [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.

[8] I also recognized that the requirements I identified may give rise to additional costs and delays associated with obtaining BII warrant powers in relation to telephone numbers or electronic identifiers that may come to CSIS's attention during the course of its investigations, and that are not linked to an identified target of investigation. Having regard to the adverse implications that the potential delays might have for CSIS's ability to investigate threat-related activities, I stated that the Court would remain open to considering alternate approaches that are *Charter* compliant: *X (Re)*, above, at para 109.

[9] In this regard, I proceeded to suggest that the additional costs and delays that may be associated with making *Charter*-compliant applications for BII warrant powers might be considerably reduced in two ways.

[10] The first way would be by providing the Court with essentially the same information that CSIS officers already provide, in their internal [redacted] forms, when they seek authorization within CSIS to request BII powers from this Court. This information describes the nexus between CSIS's investigation into a threat posed to the security of Canada and the telephone numbers or electronic identifiers in respect of which an intelligence officer would like to obtain BII. I suggested that it might be possible to provide such information [redacted] **Nexus Information**] to the Court in the form of supplementary affidavits,

filed in support of periodic requests for a proposed amendment to an existing warrant. However, after obtaining the benefit of submissions from the *amici curiae*[1] in one of the subsequent proceedings described below, I expressed three serious concerns that are more fully described in the paragraphs below. The first pertained to a potential practice of seeking "routine" amendments to previously issued BII warrants. The second related to whether CSIS can rely on a ministerial approval provided in respect of a prior request for BII warrant powers, when seeking such powers in respect of newly discovered telephone numbers or electronic identifiers. The third pertained to whether designated judges of this Court have the jurisdiction to amend each other's warrants.

[11] As a result of the foregoing concerns that I expressed, CSIS has represented that, for the "foreseeable future", it will bring fresh applications, supported by documentation that is either required by the *Charter* or appears to be contemplated by the Act, each time it seeks an authorization to obtain BII information from a CSP. The latter documentation includes a new designation and approval of the Minister of Public Safety and Emergency Preparedness [the **Minister**], as contemplated by subs. 21(1) of the Act, and a new consultation with the Deputy Minister, as contemplated by subs. 7(2) of the Act. Once again, this will be further discussed below.

[12] Given that such documentation was provided in the present proceeding, I granted the BII warrant power that CSIS sought. At that time, I also informed CSIS and the Attorney General's

[1] Mr. Gordon Cameron and Mr. Owen Rees [the ***Amici***]. They were also each appointed *amicus curiae* in X (Re), above.

representatives that I would be issuing these reasons to explain to the public why the BII warrant power which had not been granted in *X(Re)*, above, had been granted in this application.

[13] The second way in which I suggested that costs and delays might be reduced would be by simply adding the [redacted] Nexus Information to the more general information that CSIS provides to the Court regarding the relevant threat to the security of Canada, when it seeks BII warrant powers in relation to that threat: *X (Re)*, above, at paras 110-111. In the case of the threat posed by Islamist terrorism,[2] although this general information is updated from time to time to reflect relevant developments, the bulk of it has remained essentially the same since the applications that were the subject of my decision in *X (Re)*, above. This information has provided the basis for the affiant's knowledge and belief concerning the threat posed by Islamist terrorism, and has been set forth in either the main body of the affiant's affidavit or in one or more of the exhibits to that affidavit. In the latter case, the affiant has attested to his or her personal belief that the information in those exhibits is accurate**.** CSIS and the Court continue to have exchanges regarding the format in which the affiant provides this general information to the Court.

II. Developments since *X (Re)*

[14] Subsequent to the issuance of my decision in *X (Re)* last Fall, the general approach that CSIS and the Attorney General will follow in the future when seeking BII warrant powers that are unconnected with particular targets of investigation was established over the course of four applications: two in **Case B** one in **Case C** and the present application **Case D**

[2] In the recent applications that CSIS has brought to the Court seeking authorization to obtain BII in connection with its investigation into Islamist terrorism, it has defined "Islamist terrorism" to mean "activities in paragraph (c) of the definition of 'threats to the security of Canada' found in section 2 of the Act that are inspired by a violent interpretation of [redacted] Islam, including activities of the groups listed in Schedule 1**."**

[15] Given my past involvement with CSIS's request for BII warrant powers and related powers that CSIS has sought in the past (see *X(Re)*, above at paras 17-23), I presided over the above-mentioned applications and the related motions discussed below.

A. [redacted]

[16] [redacted] was characterized by counsel as an initial "test case," following my decision in *X (re)*, above. As such, it was limited in scope, and appeared to be designed to establish the basic requirements of an application for a BII warrant. CSIS simply sought authorization to obtain BII in respect of [redacted] It was a fresh application, accompanied by the required ministerial approval and designation, together with the required confirmation that the Deputy Minister had been consulted. In the initiating Notice of Application, dated [redacted] the Attorney General of Canada [**Attorney General**] stated that the grounds for the application included the affiant's reasonable grounds to believe that a warrant was required to enable CSIS to investigate Islamist terrorism.

[17] With respect to the threat to the security of Canada posed by Islamist terrorism, the affiant provided essentially the same information that he had provided in [redacted] which was one of the two applications at issue in *X (Re)*, above**.**

[18] With respect to the required nexus between, on the one hand, the [redacted] and on the other hand, CSIS's investigation into Islamist terrorism, CSIS provided the brief [redacted] Nexus Information discussed at paragraph 10 above. Ultimately, I issued the requested warrant, after satisfying myself that the requisite nexus had been

established. That is to say, I issued the warrant after satisfying myself that CSIS's affiant had provided sufficient facts to justify the belief, on reasonable grounds, that the individuals behind **electronic identifier(s)** in question either may be involved in the threat posed to the security of Canada by Islamist terrorism, or may be able to provide information to assist CSIS' investigation into that threat. Those facts were provided in the affiant's affidavit and during oral testimony at the hearing of the application. Of course, I also satisfied myself as to the other matters set forth in paragraphs 21(2)(a) and (b) of the Act, as required by subsection 21(3).

[19] Before signing the warrant sought in **Case B** I requested a change to Condition 3. As initially proposed by the Attorney General, it stated as follows:

> Any information obtained by the Service through the execution of this warrant, other than basic identifying information described in paragraphs 1 to 3, shall be destroyed within 6 months of its receipt by the Service.

[20] Upon first reading, it appeared to me that Condition 3 had been inserted to address the concern that I had identified in *Re (X)*, above, at paras 75, 87 and 100, regarding the retention of BII information pertaining to the communications accounts of third parties who have no nexus whatsoever to Islamist terrorism. That is to say, persons in respect of whom the reasonable grounds described in paragraph 21(2)(a) have not been identified to the Court.

[21] However, counsel clarified that Condition 3 was designed to address something quite different, namely, the situation in which a CSP provides more information to CSIS than simply BII. As explained by counsel, when requested to provide BII pursuant to a warrant issued by this Court, CSPs sometimes electronically transfer files that include more than BII. For example,

[redacted]

[22] Based on the foregoing explanation, I changed the six month period to four months, and signed the warrant. I also requested counsel to return to the Court within one month with language that would make it clear that BII or other information pertaining to "third parties," as described in paragraph 20 above, would be destroyed as soon as CSIS determines that it belongs to such a person. As a result of subsequent exchanges, that condition in the most recently issued BII warrants read as follows: "Any information obtained by the Service through the execution of this warrant, other than basic identifying information described in paragraph 1, shall be destroyed as soon as possible and, in all instances, within 4 months of its receipt by the Service".

B. *Amendment to warrant issued in* [redacted]

[23] On [redacted] less than two weeks after I issued the warrant described immediately above, CSIS brought an urgent motion, supported by a supplementary affidavit sworn by the same affiant, to amend the warrant that I had issued in [redacted] In brief, CSIS sought to expand that warrant to include [redacted]

[redacted]

[24] [redacted]

Case B A description of the association of the electronic identifier with the threat and the timing of the application

[redacted]

[25] Upon satisfying myself that CSIS's affiant had provided reasonable grounds to believe that a warrant to obtain BII information in respect of Electronic identifier(s) question was required to enable CSIS to investigate the threat to the security of Canada posed by Islamist terrorism, I amended by hand the warrant that I had previously issued, to include the additional Electronic identifier(s) I did so pursuant to Rule 399(2)(a) of the Federal Courts Rules, SOR/98-106 [the ***Rules***], which provides that, on motion, the Court may set aside or vary an order by reason of a matter that arose or was discovered subsequent to the making of the order.

[26] At that time, having had the benefit of submissions from the *Amici*, I also manually struck out certain language from the warrant. In essence, that language permitted CSIS to obtain BII from CSPs in a particular type of emergency situation, provided that CSIS advised the Court, in writing, within 48 hours of obtaining such BII, and seeks instructions from the Court.

[27] I will pause to note that this motion to amend the BII warrant that I had previously issued was not accompanied by a fresh Ministerial authorization or a fresh confirmation by the Deputy Minister stating that he had been consulted in respect of the motion. However, the ministerial authorization that had been provided in support of the main application in [redacted] stated that it applied to that application as well as to "subsequent requests for judicial authorization to obtain BII." Although the *Amici* expressed concerns about the nature of that authorization, the urgency of the situation was such that they supported the Attorney General's request for the amendment in question. They did so on the express understanding that the issue of the open-ended nature of the Minister's authorization, dated [redacted] would be revisited in the near future.

C. *Additional Application in* [redacted]

[28] On [redacted] CSIS filed another application for an authorization to obtain BII in respect of [redacted] That application was supported by a new affidavit, a new Ministerial authorization and designation, and a new confirmation that the Deputy Minister had been consulted.[3] As such, it did not give rise to some of the difficulties that arose in some of the subsequent proceedings, described below.

[29] Once again, the affidavit, as amended immediately following the hearing of the application, contained essentially the same general information with respect to the threat posed by Islamist terrorism as had previously been provided by CSIS, both in support of its initial

[3] Given these facts, the application ordinarily would have been given a new Court file number.

application in **Case B** and in one of the applications **Case A** that was the subject of *X(Re),* above.

[30] In addition, the affidavit, supplemented by the affiant's testimony, provided sufficient facts pertaining to the nexus between, on the one hand, the above-mentioned Electronic identifier(s) and on the other hand CSIS's investigation into the threat posed to the security of Canada by Islamist terrorism, to provide the reasonable grounds to believe that are contemplated by subs. 21(3) of the Act and the *Charter*.

[31] Given the foregoing, and upon satisfying myself as to the other matters contemplated by subs. 21(3), I granted the further warrant that CSIS sought.

D. *Motion to further amend the warrant issued in* **Case B**

[32] On the Attorney General filed a motion to vary the initial warrant issued in **Case B** In that motion, the Attorney General sought Electronic identifier(s) that had been brought to its attention subsequent to when I made the initial amendment to the first warrant I issued in **Case B** The motion was supported by an affidavit that provided essentially the same general information as had previously been provided to the Court regarding the threat posed by Islamist terrorism, together with Nexus Information to establish the requisite nexus between that threat and each of the new Electronic identifier(s).

[33] In support of the motion, the Attorney General provided written submissions. Those submissions were addressed toward the following three legal issues that the Attorney General maintained were raised by the motion:

i. *Whether the Federal Court has the authority to issue warrants that contemplate the granting of further authorizations with respect to BII, when specifically authorized by the Court at the time such further authorizations are sought;*

ii. *Whether the BII warrant, as amended on November 16, 2017, may be varied pursuant to Rule 399(2)(a) or Rule 4 of the Rules; and*

iii. *Whether the affidavit filed in support of the motion contained sufficient information to enable the Court to understand the nexus between the persons whose privacy interests may be encroached and the threat-related activities that are the focus of the CSIS investigation into Islamist terrorism.*

[34] The *Amici* recast these issues in the following way:

i. *Does the Director (or the Director's designate) need to consult with the Deputy Minister and obtain the approval of the Minister before applying to the Court for new BII authorizations?*

ii. *Can new BII searches be authorized pursuant to a motion to vary under Rule 399(2)(a)?*

iii. *Does the affidavit evidence filed in support of the motion to vary meet the standard required under s. 21 of the Act and s. 8 of the Charter for the issuance of a BII warrant?*

[35] For the purposes of the summary provided below, I will use the statement of the issues provided by the *Amici*.

[36] Given that the Attorney General ultimately withdrew the motion, I will refrain from taking a definitive position on those issues.

(1) Does the Director (or the Director's designate) need to consult with the Deputy Minister and obtain the approval of the Minister before applying to the Court for new BII authorizations?

[37] The Attorney General submitted that the requirement in subsection 21(1) that the Minister approve the making of warrant applications does not apply to a motion to vary the BII warrant that I had previously issued, by simply expanding it to include additional [redacted] Electronic identifier(s)

[38] In the Attorney General's view, the principle of ministerial accountability that underpins the ministerial approval requirement in subsection 21(1) does not require the Minister to authorize the intrusion into the reasonable expectation of privacy of each and every person that may take place pursuant to a warrant issued under that provision of the Act. Instead, the Minister is simply required to approve *the extent of the intrusive powers to be sought from the Court*, after assessing both the nature of the relevant threat to the security of Canada and the scope of the privacy concerns or intrusions that are contemplated by the requested warrant. The Attorney General maintained that Minister had already provided such approval, and conducted those two assessments, immediately before the Attorney General sought the initial BII warrant from this Court, in [redacted]

[39] Stated differently, the Attorney general asserted that the subject of the warrant was Islamist terrorism, and that the Minister had already assessed the nature of the threat posed by Islamist terrorism, as well as the narrow scope of the privacy concerns raised by an authorization to obtain BII in respect of communications accounts, at the time the initial BII authorization was sought, in [redacted]

[40] The *Amici* disagreed. In their written submissions they maintained that subsection 21(1) makes the Minister accountable for each intrusion upon the reasonable expectation of privacy of a person. They asserted that the text, the scheme and the legislative history of the Act all support the conclusion that, to properly perform his mandate under s. 21 of the Act, the Minister must understand the factual nexus between the relevant threat to the security of Canada and the person(s) whose privacy interests will be intruded upon. Viewed from this perspective, each intrusion into the privacy interests of each additional person constitutes a new "search." Moreover, the subject of the warrant is the person whose privacy interests would be intruded upon, rather than the threat posed by Islamist terrorism. The *Amici* emphasized that to permit the Minister to grant a blanket authorization in respect of a broad threat such as that posed by Islamist terrorism would effectively and impermissibly delegate to the Director or another designated employee of CSIS the decision as to whether to apply for a warrant.

[41] Subsection 21(1) of the Act states as follows:

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

(2) to a judge for a warrant under this section.	en vertu de l'article 16.

[42] In support of their position, the *Amici* referred to two important aspects of the legislative history of the Act, namely, (i) the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Policy, Second Report – Volume 1. *Freedom and Security Under the Law*. *Ottawa*: 1981 [the **McDonald Commission Report**], and (ii) some of the statements that were made by the responsible Minister when Bill C-9, which became the Act (after certain amendments were made), was before the House of Commons Justice and Legal Affairs Standing Committee [the **Committee**].

[43] Concerning the McDonald Commission Report, the *Amici* referred to a number of passages. This included the following:

> 32. […] The decision to subject an individual or group to any or all of these techniques for national security purposes is a decision with important policy implications which in our view ought to have the approval of a responsible Minister. […]
>
> 33. […] As we see it, the ministerial role with respect to these powers is to make policy decisions. For example, the Minister must decide whether the activities of a certain country's diplomats are sufficiently suspect and dangerous to risk the diplomatic repercussions of possible exposure of security intelligence surveillance, or whether the activities of a violence-prone group pose a sufficient threat to the country's democratic process to warrant deploying the full investigative resources of the security intelligence agency. It is primarily questions of this kind which the Solicitor General must consider in deciding whether to approve an application for a judicial warrant. He might refuse to authorize an application even though convinced that it met the statutory standard. The Solicitor General should by no means be indifferent as to whether the legal requirements were satisfied by a proposed application: on the contrary, he should not approve the application for a judicial warrant unless satisfied that the legal requirements

have been met. However, our proposals give the judiciary, not the Minister (or his legal advisers), the final decision whether the law is being properly applied. In our view this would ensure the application of the rule of law to these aspects of security intelligence operations and does not depart from the appropriate distribution of responsibilities between Ministers and judges.

34. In the system we propose, at the same time that the Minister gives his general approval to a proposal to initiate a full investigation he may also approve a proposal to apply for a judicial warrant to use one or more particular techniques. He might, however, not be asked for such approval or might withhold it until other techniques not requiring a judicial warrant have been used.[4]

[…]

101. First, it might be argued that the question of whether an individual or group constitutes a sufficient threat to national security to justify an electronic intrusion should be decided by Ministers who, unlike judges, are accountable to Parliament and ultimately to the electorate for national security policies. We agree with part of this argument. Ministers are responsible for the national security activities of government; in particular, the Solicitor General, as the Minister responsible for the security intelligence agency, is responsible for the investigative policies and practices of that agency. That is why we think the Solicitor General should approve proposals by the agency to use electronic surveillance (and other intrusive techniques). He should approve such proposals from a policy point of view. But he and the Cabinet must discharge their responsibility for national security policy within the law. When the law establishes a carefully defined standard for exercising an investigative power which would otherwise be a criminal offence, there is, in our view, no derogation of ministerial responsibility in denying Ministers the final authority to determine whether a particular case meets that standard. Our system of government is not based on the single principle of ministerial responsibility: it involves other important principles, one of which is the rule of law. In a system of responsible Cabinet government operating within the rule of law Ministers are responsible for the effective and proper execution of the powers lawfully available to government, but they do not have the final responsibility for determining what the law is. In our system of government this is normally the function of judges.

[4] Canada. Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police. Second Report. *Freedom and Security Under the Law*. Ottawa: The Commission, 1981), pp. 525-26.

> 102. We should emphasize that we are not suggesting that the Minister should be indifferent as to whether a proposal to employ electronic surveillance meets the legal requirements. On the contrary, he and his advisers should thoroughly scrutinize proposals from a legal as well as a policy point of view before approving an application for a judicial warrant. But our review of the administration of section 16 of the Official Secrets Act has indicated to us that there is not sufficient assurance that in every case Ministers will carefully and judiciously apply their minds to all of the legal requirements for the use of this extraordinary power. We think that judges are more apt to have the appropriate experience and to be operating in an appropriate setting for making that kind of determination of the law. As we argued earlier, normally the courts determine the legality of government action only when it is challenged after the fact. However, because the effective use of this power should always be secret, no such *ex post facto* challenge is possible by persons who may be subject to an unlawful exercise of the power. Therefore, we think it necessary that a judicial determination of lawfulness be made before the power is exercised.[5] [Emphasis added.]

[44] With respect to statements made by the relevant Minister (the Solicitor General) when Bill C-9 was before the Committee, the *Amici* noted that the Solicitor General rejected the recommendation of the Senate that the Bill include a clause permitting the Court to assess the gravity of the threat, as apparently was the case in the United States. In this regard, the Solicitor General explained as follows:

> **Mr. Kaplan:** I did not agree with the recommendation because I felt that what the judge was being asked to do in that case was not to make a judicial decision about protecting the rights or privacy of an individual, but to decide on the importance of a national security matter, and that that was a matter that should be left to the government and one for which the government should be responsible.
>
> If the government is of the view that a matter is important enough to justify surveillance, we did not want the judge to have to have that decision about how important it was. The judge makes the decision about whether other methods are available, whether the

[5] *Ibid*. at p. 556 [emphasis added].

> belief is reasonable or probable, to add that matter, whether the warrant should be long, whether additional terms and conditions should be imposed, but the fundamental question of whether the national security justifies that application to be made is not something that we wanted… It is just not within the judging responsibility to make a decision like that. The government ought to make a decision like that. The government ought to be responsible for determining the gravity of the matter in terms of national security. [Emphasis added]
>
> *House of Commons, Minutes of Proceedings and Evidence of the Standing Committee on Justice and Legal Affairs respecting Bill C-9, 32nd Parl, 2nd Sess, Issue No 29, at 32.*

[45] The Solicitor General proceeded to emphasise the importance of requiring the Minister to approve every warrant:

> **Mr. Robinson (Burnaby):** Surely that significantly dilutes the significance of the judicial intervention in the process of the granting of warrants. In effect, what the Minister is saying is that the judge will have to grant the warrant unless these other techniques are available.
>
> **Mr. Kaplan:** Do you mean unless he does not believe that there is reasonable evidence? But weighing evidence and assessing alternatives are judicial functions. Considering whether the national security is affected or not is a matter for the government.
>
> This was a point in which we went further than the Pitfield committee, recognizing their concern on that issue, and that is to require the Minister to approve every warrant. The Senate was content with a process in which warrants could be sought without the approval of the Minister. The court, in a sense, was assigned the Minister's function of assessing gravity. What we have in the Bill is that the Minister assesses the gravity and approves of a warrant if he feels that the game is worth the candle. The court then has all the other responsibilities that the Senate committee wanted it to have. [Emphasis added]
>
> *Minutes of Proceedings and Evidence of the Standing Committee on Justice and Legal Affairs respecting Bill C-9, 32nd Parl, 2nd Sess, Issue No 29 (May 29, 1984), at 32.*

[46] In Reply to the *Amici*, the Attorney General noted that the Solicitor General subsequently stated the following in response to concerns regarding the assistance power in s. 16 of the Bill:

> I want to reassure them by pointing out that activity under this clause requires the highest level of approval. It requires approval by Ministers of the Crown accountable to Parliament. I think in our system of government that is the best safeguard you can have - if you are asking for the power, and we are asking for the power.
>
> I am reminded by my deputy that warrants are needed from judges for this, too. So there is not only the control of accountable Ministers who have to seek it but also a judge who has to be satisfied that the invasion of privacy which a warrant is justified. [Emphasis added]
>
> *Minutes of Proceedings and Evidence of the Standing Committee on Justice and Legal Affairs respecting Bill C-9, 32nd Parl, 2nd Sess, Issue No 38 (June 7, 1984), at 59*

[47] The Attorney General maintained that the underlined passage in the quote immediately above makes it clear that it is a judge of this Court, rather than the Minister, who has to weigh the intrusion on an individual's privacy rights against the interest of the state in obtaining particular warranted powers that may be sought before this Court.

[48] However, during the hearing, I questioned whether subs. 21(1) contemplated that CSIS could return to the Court, perhaps on a weekly basis, to seek amendments to a warrant based on a single ministerial approval provided to the Court at the time of the initial warrant application. I observed that such a process could result in expanding a BII warrant over time to include what could ultimately amount to potentially many more telephone numbers or electronic identifiers. In this regard, I queried how the Minister could be accountable if he had no idea how many times CSIS might seek to expand the BII authorization in a warrant, or how many individuals might ultimately wind up having have their privacy interests intruded upon.

[49] I also questioned how such an expansion of warrant powers without a fresh approval from the Minister could be consistent with the *Ministerial Direction for Operations and Accountability*, approved by the Minister on [redacted] [the **Ministerial Direction**]. Among other things, Annex B to that document stipulates that CSIS "will seek the approval of the Minister for any changes that substantially alter the application occurring after the Minister has approved the application," including:

- Changes to the subject(s) of the warrant, and the supporting justification;
- Changes to the length of time for which any of the requested warrants are proposed to be in force and the supporting justification; and
- Additions to the list of places where the warrant may be executed and the supporting justification, if the request is in relation to a Canadian fundamental institution.

[50] With regard to the foregoing, counsel to the Attorney General struggled to explain why the Minister would insist on approving changes to the manner in which a warrant might be executed (i.e., changes to the length of time of the warrant and to the list of places where it might be executed), but would not insist upon approving potentially significant expansions to the number of persons whose privacy interests might be intruded upon, where the nexus between those individuals and the investigation in question has not been established in advance.

[51] I will simply add that counsel to the Attorney General did not provide any evidence regarding the difficulty that might be associated with obtaining ministerial approval prior to CSIS seeking to expand a BII warrant to include additional telephone numbers or electronic identifiers.

(2) Can new BII searches be authorized pursuant to a motion to vary under Rule 399(2)(a)?

[52] The Attorney General submitted that Rule 399(2)(a) can be relied upon to vary the BII warrant that I initially issued in [redacted] and amended the following month. She maintained that it would be open to the Court to vary that warrant as soon as the Court was satisfied that the required nexus had been established between its investigation into Islamist terrorism and the individuals whose privacy rights would be intruded upon.

[53] Rule 399(2) states as follows:

399. (2) On motion, the Court may set aside or vary an order	**399. (2)** La Cour peut, sur requête, annuler ou modifier une ordonnance dans l'un ou l'autre des cas suivants :
(a) by reason of a matter that arose or was discovered subsequent to the making of the order; or	**a)** des faits nouveaux sont survenus ou ont été découverts après que l'ordonnance a été rendue;
(b) where the order was obtained by fraud.	**b)** l'ordonnance a été obtenue par fraude.

[54] The Attorney General added that the Court should approach its interpretation of Rule 399(2)(a) through the lens of Rule 3, which provides:

3. General Principle – These Rules shall be interpreted and applied so as to secure the just, most expeditious and least expensive determination of every proceeding on its merits.	**3. Principe général** – Les présentes règles sont interprétées et appliquées de façon à permettre d'apporter une solution au litige qui soit juste et la plus expéditive et économique possible.

[55] In support of her position in respect of Rule 399(2)(a), the Attorney General maintained that the newly discovered Electronic identifier(s) constituted newly discovered "matters," as contemplated by that Rule, which were not discoverable prior to the making of the initial BII warrant. She submitted that those matters had a determining influence on the decision the Court was being asked to make: *Ayangma v Canada*, 2003 FCA 382, at para 3. After recognizing that the exceptional nature of the relief contemplated by Rule 399(2)(a) (*Saywack v Canada (Minister of Employment and Immigration*, [1986] 3 FC 189, at para 14 [***Saywack***]), she asserted that the relief being sought in the motion was exceptional in nature.

[56] In the alternative, the Attorney General took the position that Rule 4, also known as the "gap rule" could be relied upon. Rule 4 states:

Matters not provided for	**Cas non prévus**
4 On motion, the Court may provide for any procedural matter not provided for in these Rules or in an Act of Parliament by analogy to these Rules or by reference to the practice of the superior court of the province to which the subject-matter of the proceeding most closely relates.	**4** En cas de silence des présentes règles ou des lois fédérales, la Cour peut, sur requête, déterminer la procédure applicable par analogie avec les présentes règles ou par renvoi à la pratique de la cour supérieure de la province qui est la plus pertinente en l'espèce.

[57] The *Amici* took issue with the Attorney General's characterization of the motion as involving a request to vary the pre-existing BII warrant issued in Case B In their written submissions they maintained that, in substance, the Attorney General was applying for new judicial authorizations to search, which constitute the very heart of a warrant application. In their

view, it was never contemplated that Rule 399(2) might be used to authorise entirely new searches that intrude upon the privacy interests of individuals who were not contemplated by a prior warrant. Rather, the Act requires a new warrant application for each intrusion on the privacy interests of such an individual.

[58] During the hearing, I pressed the Attorney General's representative on whether Rule 399(2)(a) could be used to support what may become a routine process in which CSIS might seek to add, on multiple occasions, new electronic identifiers or telephone numbers to a previously issued BII warrant. I queried how this would be consistent with the exceptional nature of that Rule, which the Attorney General had acknowledged.

[59] I also queried whether subs. 21(3) provides jurisdiction to the Court's designated judges to amend each other's warrants. This was an important issue because the Attorney General was endeavouring to establish an efficient process that could be used to permit any designated judge who may happen to be on duty to expand the initial BII warrant that I had previously granted.

[60] In this regard, the relevant language of subs. 21(3) states as follows:

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	**(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

authorizing the persons to whom it is directed to intercept any communication or obtain any information, record, document or thing and, for that purpose,	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.
[Emphasis added.]	[Non souligné dans l'original.]

[61] Notwithstanding the foregoing wording in subs. 21(3), the Attorney General maintained that in a motion under Rule 399(2)(a) any designated judge of this Court can amend a warrant previously granted by another judge. In her view, that may be done without the need for a new application and its associated requirements (including a new ministerial approval). The designated judge seized with such a motion would simply have to be satisfied that the requisite nexus between CSIS' investigation and the new electronic identifier(s) or telephone number(s) had been established. The Attorney General added that Rule 399(2) explicitly allows "the Court" to set aside or vary an order. In response to my query as to whether any inconsistency between

that Rule and subs. 21(3) should be resolved in favour of the latter, the Attorney General maintained that the Act is silent on who should be allowed to amend a warrant, such that Rule 399(2)(a) can be relied upon.

[62] With respect to Rule 4 (the "gap" rule), I queried whether there was anything in the Rules of Ontario or another province which supported the Attorney General's position that a warrant issued by a particular judge of a Court could be amended by another judge of that Court. Counsel replied in the negative.

(3) Abandonment of Motion

[63] Immediately following the exchanges summarized above, and before addressing the third issue identified at paragraph 34 above, the Attorney General's representative requested a short break. She returned a short while later to request an adjournment of her motion.

[64] She did so after I had questioned the soundness of the legal foundation that had been advanced in the motion. After underscoring once again the problematic nature of the issues concerning ministerial approval, Rule 399(2)(a) and the jurisdiction of designated judges to amend each other's warrants, I observed that I did not have the mental image of a solid foundation upon which to move forward with regular BII authorizations in the future.

[65] The following week, the Attorney General filed a Notice of Abandonment in respect of the motion.

E. **Case C**

[66] On [redacted] the Attorney General filed a new application for authorization to obtain BII in respect of **Electronic identifier(s)** That application was supported by an affidavit that provided (i) essentially the same information with respect to the threat posed to the security of Canada by Islamist terrorism that had been provided to the Court in **Case B** (ii) [redacted] Nexus Information to establish the nexus between CSIS's investigation into that threat and the **Electronic identifier(s)** in question, (iii) the facts relied upon to justify the belief, on reasonable grounds, that a warrant was required to enable CSIS to investigate that threat, and (iv) the facts relied upon to satisfy the Court as to the matters referred to in subs. 21(2)(b) of the Act.

[67] In addition, that application was supported by a ministerial approval and designation of the applicant affiant, as well as confirmation by the Deputy Minister that she had been consulted with respect to the application.

[68] Based on the foregoing, it appeared that the basic framework within which BII warrants would be sought from the Court had been established. Indeed, at the outset of the hearing on **Case C** the Attorney General's representative stated his understanding that, "for the time being, at least, my understanding is the Service will obtain the designation and approval from the Minister and will consult the Deputy Minister on each of these applications for … BII."

[69] Consequently, my understanding was that the focus of BII warrant applications going forward would be upon the matters described in points (ii) – (iv) of paragraph 66 above. With

respect to CSIS' investigation the threat posed to the security of Canada by Islamist terrorism, I understand that CSIS may bring applications for BII authorization on a regular, perhaps, monthly basis.

[70] Based on information provided on behalf of the Attorney General, I further understand that there are legitimate operational reasons why more frequent applications typically cannot be made. With this in mind, I noted that the Court would remain open to continued exchanges with the Attorney General regarding a potential process for addressing urgent situations when a BII authorization might be required during the period of time between two "routine" applications. In this regard, I suggested that, depending upon the circumstances, the Court might be prepared to provide such an authorization by way of an amendment to an existing warrant. Of course, the Court would have to be satisfied that the circumstances in question were of the "exceptional" nature contemplated by the jurisprudence: *Saywack*, above. In addition, prudence would dictate that the Attorney General keep in mind the issues that have been identified with respect to ministerial approval and the specific reference to "the" judge, in subs 21(3) of the Act.

[71] There is one further aspect of **Case C** that merits addressing here. During the *en banc* hearing in *X (Re)*, above, the Court expressed concern about the possibility that CSIS might seek authorization to obtain BII in respect of [redacted] In recognition of that concern, the Attorney General's representative underscored that the electronic identifiers in respect of which an authorization to obtain BII had been sought were not those of

individuals who might simply have been [redacted]

[72] I was persuaded that this was unlikely to be the case, after the affiant satisfied me that [redacted] Based on the foregoing facts, I was satisfied that the Attorney General had demonstrated the required nexus between the electronic identifiers in question and CSIS's investigation into the threat posed to the security of Canada by Islamist terrorism. I was also satisfied that there were reasonable grounds to believe that a warrant authorizing CSIS to obtain BII in respect of the electronic identifiers was required to enable CSIS to pursue that investigation. In this regard, I was satisfied that there were reasonable grounds to believe that the individuals behind the electronic identifiers either (a) may themselves be involved in threat-related activities, within or relating to Canada, or (b) may be in a position to provide information that could assist CSIS to advance its investigation.

[73] Contrary to the submissions of *Amici*, I did not consider that it was necessary for the affiant to provide reasonable grounds to believe that the persons behind the electronic identifiers were actively contributing [redacted] In my view, the mere fact that they [redacted] put them in a position to potentially provide information that might

assist CSIS to advance its investigation. I also did not consider it to be necessary that they [redacted] Indeed, it is in part due to the uncertainty in this regard that CSIS needed to be able to obtain BII, [redacted]

F. *Motion in* **Case C**

[74] On [redacted] less than three weeks following the hearing of the application in **Case C** [redacted] the Attorney General brought a motion to vary the BII warrant that I had granted. In brief, the Attorney General sought to add **Electronic identifier(s)** to the warrant. The Attorney General's representative explained that the **Electronic identifier(s)** was discovered after the warrant was issued, and that the circumstances were such that CSIS could not wait until the next [redacted] application. He added that the Attorney General and CSIS were still attempting to develop a process for dealing with such time sensitive applications, having regard to the concerns that I had previously expressed. With that in mind, he took the position that the motion would address the "watershed" issue of when a motion to vary, versus a new application, may be filed.

[75] The circumstances in question were as follows: [redacted]

[redacted]

CSIS learnt of information supporting an urgent need to obtain BII associated with an electronic identifier(s)

in relation to a serious threat – related matter (ref paragraph 75 + 76).

[redacted]

[76] **The CSIS affiant explained the timing of the application**

[redacted]

[77] The affiant stated that he considered the foregoing information to be very credible and that a warrant authorizing CSIS to obtain the BII associated with the **Electronic identifier(s)** was "required to urgently [redacted]

[78] The Attorney General took the position that this Court had the jurisdiction to grant the motion based on the existence of "exceptional" circumstances, as required by the jurisprudence under Rule 399: *Saywack*, above. Those circumstances were stated to be: (i) the "pressing" nature of the matter, (ii) the fact that it was the top priority of CSIS's [redacted] (iii) the fact that it was [redacted] and (iv) the request was "unique." These circumstances were contrasted with the "routine" nature of the monthly requests for BII authorizations, in respect of which I expressed concerns during the hearing of the motion in [redacted] discussed in part II.D. above. Counsel disclosed that the latter motion had been abandoned based on the concerns that I had identified regarding the use of Rule 399(2)(a) to bring "routine" monthly motions to vary a warrant, and regarding the jurisdiction of a designated judge of this Court to amend a warrant granted by another designated judge, given the language in subs. 21(3), discussed at paragraphs 59-60 above.

[79] Notwithstanding the foregoing, and notwithstanding the view of the affiant and the abovementioned [redacted] that the matter was "urgent," counsel underscored that CSIS was not taking the position that the circumstances were so urgent as to prevent the Minister from giving his approval for the motion.

[80] Given the combination of the four circumstances described at paragraph 78 above, the Attorney General's position was that the approval of the Minister was not required. For this reason, the Minister's office was simply "advised of this motion." Neither the affiant nor counsel knew whether the Minister himself had been advised of the motion. However, counsel observed that based on his past dealings with the Minister's office, "if they did not want the Service to be

here, we would not be here today." Counsel added that the Minister did not personally need to approve the motion for the following three reasons:

i. I had already issued a BII warrant in this proceeding [redacted]

ii. CSIS was simply seeking to exercise the same BII power that I had previously authorized; and

iii. the affiant was providing the information required for me to satisfy myself as to the nexus between the [redacted] and CSIS's investigation into the threat to the security of Canada posed by Islamist terrorism.

[81] With respect to the first of the three points immediately above, counsel to the Attorney General emphasized that the Minister's approval was unnecessary because I had already granted a warrant in respect of the above-described threat posed by Islamist terrorism.

[82] I pause to add that the affiant disclosed during cross-examination that [redacted]

[83] The *Amici* disagreed with Attorney General's position regarding my jurisdiction to amend the warrant that I had issued on [redacted] They did so for two reasons: First, relying on my decision in *X (Re)*, above, at paras 6 and 61, they maintained that a fresh warrant is required each time CSIS seeks to intrude upon the privacy interests of a person who is not already the subject of a warrant, or each time CSIS seeks powers to extend its intrusion into an individual's

privacy interests, in a "serious" manner. In this latter regard, and in response to my questioning, the *Amici* stated that a fresh warrant would be required to add to an existing warrant [redacted] but that a fresh warrant would not be required to add [redacted] in respect of which a BII warrant had already been issued by the Court.

[84] The *Amici* explained that with respect to the number of [redacted] a request for authorization to obtain BII would constitute a new "search," within the meaning of the jurisprudence that has developed under the *Charter*: see generally *X (Re)*, 2017 FC 1047, at paras 110-124. The same would be true for a request to obtain BII in respect of a newly discovered telephone number or electronic identifier, which belonged to an individual who had not been the subject of the balancing analysis required by the *Charter*, at the time the initial BII warrant was granted.

[85] The second reason why the *Amici* maintained that I did not have the jurisdiction to amend the BII warrant that I had previously issued is that the legislative history discussed at paragraphs 42-46 above reflects Parliament's intention that the Minister consider whether the state's interest in obtaining BII in respect of that number outweighs the individual's privacy interest in that BII. Accordingly, in the absence of the ministerial approval contemplated by subsection 21(1) of the Act, this Court has no jurisdiction to issue or amend a warrant that would permit CSIS to intrude upon an individual's privacy interests. Moreover, they maintained that the legislative history of the Act also reflects Parliament's intention that prior Ministerial approval

be given even in emergency situations. In this regard, the *Amici* drew my attention to the following passages from McDonald Commission Report, above:

> 27. We believe that decisions to subject an individual or the members of an organization to any of the techniques listed above are so important, in terms of both the effective deployment of the security agency's resources and the potential impact on civil liberties, that they should be based on evidence that meets a standard defined by statute. Except in emergency circumstances, such decisions should be approved by the Solicitor General, as the Minister responsible for the agency. We should make it clear that the decisions we refer to here are the ones that determine that evidence obtained through less intrusive techniques of investigation justifies intensifying the general level of investigation to the most intrusive stage. Particular techniques of investigation may require an additional level of authorization. For instance, under our recommendation the use of electronic surveillance, surreptitious entry or a mail check, or access to certain kinds of confidential information, would require judicial authorization.
>
> […]
>
> 29. A procedure for emergency situations should be provided for. It should be possible for the Director General (or a person authorized in writing by the Director General to act in his place) to initiate a full investigation for 48 hours, without obtaining Stage 1 or Stage 2 approval. However, the Solicitor General's approval should have to be obtained within 48 hours. If it is not obtained, the full investigation should have to be terminated. It is understood that if the Solicitor General is absent or otherwise incapacitated, the Acting Solicitor General would be able to act in his place. The Director General should report immediately to the Minister each emergency authorization which he grants. This emergency procedure does not remove the necessity to obtain a warrant authorizing those intrusive techniques which later in this chapter we recommend require a judge's warrant. [Emphasis added.]

[86] Given that Parliament did not include in the Act, or in any regulations enacted pursuant to the Act, any such emergency procedure, the *Amici* requested me to infer that Parliament implicitly decided not to provide CSIS with the ability to seek warrants in emergency situations, without the prior approval of the Minister.

[87] With respect to the Attorney General's position that the BII warrant issued on [redacted] had been issued in respect of the threat posed by Islamist terrorism, the *Amici* underscored that "[t]here is no such thing as a threat warrant." Relying on my decision in *X (Re)*, above, at paras 58-61, they maintained that warrants are not issued in respect of threats, but rather in respect of activities that intrude on the privacy interests of specific individuals, whether or not those individuals have been identified.

[88] In the alternative, the *Amici* maintained that even if I might have jurisdiction under the Act and under Rule 399(2)(a) to amend the warrant that I had previously issued (by adding the [redacted] Electronic identifier(s) the exceptional circumstances required to invoke that Rule had not been established.

[89] In this regard, the Attorney General's representative conceded that no evidence had been adduced regarding the ability of the Minister to approve the motion, prior to the hearing. Indeed, as I have already noted, the Attorney General made it clear that she was not asserting that the Minister could not have approved the motion, but rather that such approval was not required, given the alleged "exceptional" circumstances described at paragraph 78 above.

[90] Considering the above, the *Amici* submitted that the evidence required to engage any discretion that I might otherwise have had under Rule 399(2)(a), if I had not been persuaded by the *Amici*'s other arguments, had not been provided.

[91] Having regard to all of the foregoing, I stated at the end of the hearing that I would reserve my decision on the motion until the following day. However, before I communicated that decision to the Attorney General, a Notice of Abandonment was filed, wholly abandoning the motion.

G. Case D

[92] On [redacted] CSIS brought a fresh application requesting authorization to obtain BII from CSPs in respect of Electronic identifier(s)

[93] That application was supported by a new designation and approval of the Minister, and a new confirmation that the Deputy Minister had been consulted, as contemplated by subs. 7(2) of the Act. CSIS's affiant also satisfied me as to the matters referred to in paragraphs 21(2)(a) and (b) of the Act, through her affidavit and her oral testimony during the hearing of the application. For greater certainty, this included establishing the required nexus between, on the one hand, CSIS's investigation into the threat to the security of Canada posed by Islamist terrorism, and on the other hand, the Electronic identifier(s) With one exception, I was satisfied that there are reasonable grounds to believe that the individuals behind each of the Electronic identifier(s) in question either may be involved in the threat posed to the security of Canada by Islamist terrorism, or may be able to provide information to assist CSIS' investigation into that threat. The single exception concerned Electronic identifier(s) in respect of which I did not consider that such nexus had been established.

[94] During the course of the hearing in this application Case D the Attorney General's representative advised me that the approach that had been followed in this application was "unlikely to change, at least for the foreseeable future."

III. Conclusion

[95] Based on representations made to the Court in this proceeding it appears as though an understanding has now been reached as to the basic approach that CSIS and the Attorney General will follow when seeking judicial authorization from this Court to obtain BII from CSPs in respect of one or more telephone numbers or electronic identifiers that may come to CSIS's attention during the course of an investigation. In brief, that approach is as follows:

i. A fresh application will be filed, supported by a fresh affidavit that provides the facts relied upon to satisfy this Court of the matters referred to in paragraphs 21(2)(a) and (b) of the Act. For greater certainty, those matters will include the required nexus between the relevant investigation being conducted by CSIS and the telephone number(s) or electronic identifier(s) in respect of which CSIS seeks an authorization to obtain BII. To satisfy the Court with respect to that nexus, the facts adduced by CSIS's affiant must provide reasonable grounds to believe that the individuals behind each of the Electronic identifier(s) in question either may be involved in the identified threat posed to the security of Canada that CSIS is investigating, or may be able to provide information to assist CSIS' investigation into that threat.

ii. A fresh designation and approval of the Minister, and a fresh confirmation of consultation from the Deputy Minister, will be filed in respect of each such application.

iii. In urgent situations where it is not possible to obtain the Minister's designation/approval or the Deputy Minister's the confirmation of consultation, in writing, it will suffice if the Attorney General or her representative (i) advises the Court that such designation/approval and such confirmation have been provided orally, and (ii) undertakes to provide a written designation/approval and a written confirmation of consultation as soon as is reasonably possible.

[96] Given that the information described in subparagraphs (i) and (ii) immediately above had been provided to the Court, I issued the BII warrant that CSIS had requested. In brief, by providing that information, CSIS overcame the deficiencies that were identified in *X (Re)*, above. In addition, CSIS's approach also implicitly addressed the concerns that I had expressed with respect to (a) CSIS's reliance on a ministerial approval that had been provided in respect of a prior request for BII warrant powers, (b) the practice of seeking "routine" amendments to a previously issued BII warrant, and (c) the jurisdiction of the designated judges of this Court to make amendments to each other's warrants.

[97] The Attorney General's representatives and the Court continue to have exchanges regarding the optimal format of the affidavit filed in support of applications for BII warrants. In this regard, that the bulk of the factual information provided by CSIS's affiant regarding the threat posed to the security of Canada by Islamist terrorism sometimes does not change from one month to another. Considering that practical reality, the Court recognizes that it may be more efficient for that extensive factual information to be provided in an appendix or an annex to the affidavit, rather than in the body of the affidavit itself. Of course, if CSIS's affiant decides to

proceed in the latter fashion it will be necessary for the affiant to state that the information in the appendix or annex forms part of the affidavit, and that he or she has personal knowledge of the information and believes it to be true and accurate.

[98] One of the Attorney General's representatives has expressed the hope that, at some point in the future, it may be possible for applications for BII warrants to be dealt with by the Court in writing, without the need for a hearing. Based on my experience with such applications so far, *viva voce* evidence from CSIS's affiant has been essential to satisfying me as to the required nexus between CSIS's investigation and at least some of the electronic identifiers or telephone numbers in respect of which a BII warrant has been sought. I expect that this will continue to be the case until the affiant's affidavits address the types of shortcomings that I and other designated judges of the Court have identified.

"Paul S. Crampton"
Chief Justice

FEDERAL COURT

SOLICITORS OF RECORD

DOCKET:	[redacted]
STYLE OF CAUSE:	IN THE MATTER OF AN APPLICATION BY [redacted] FOR WARRANT 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
PLACE OF HEARING:	OTTAWA, ONTARIO
DATE OF HEARING:	APRIL 9 , 2018
REASONS :	CRAMPTON C.J.
DATED:	AUGUST 30, 2018

APPEARANCES:

In Docket [redacted]	DEPARTMENT OF JUSTICE
Mr. Gordon Kirk	NATIONAL SECURITY LITIGATION
Ms. Amy Joslin-Besner	AND ADVISORY GROUP
In Docket [redacted]	DEPARTMENT OF JUSTICE
Mr. Gordon Kirk	NATIONAL SECURITY LITIGATION AND ADVISORY GROUP
Mr. Gord Cameron	*AMICI CURIAE*
Mr. Owen Rees	
In Docket [redacted]	DEPARTMENT OF JUSTICE
Mr. Gordon Kirk	NATIONAL SECURITY LITIGATION
Mr. Arlo Litman	AND ADVISORY GROUP
Ms. Nathalie Benoit	
Mr. Gord Cameron	*AMICI CURIAE*
Mr. Owen Rees	

SOLICITORS OF RECORD:

Attorney General of Canada
Ottawa, Ontario

DEPARTMENT OF JUSTICE
NATIONAL SECURITY LITIGATION
AND ADVISORY GROUP

Blakes Cassels & Graydon LLP
Barristers and Solicitors
Ottawa (Ontario)

AMICI CURIAE

Conway Baxter Wilson LLP
Barristers and Solicitors
Ottawa, Ontario