Federal Court Cour fédérale

~~**TOP SECRET**~~

Date: 20191128

Docket: CONF-2-19

Citation: 2019 FC 1359

Ottawa, Ontario, November 28, 2019

PRESENT: The Honourable Madam Justice Kane

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 [CYBER THREATS] [redacted]

REASONS

KANE, J.

I. Overview

[1] In the context of the above noted Application, the Court noted that the warrant requested would include provisions that were similar to those considered by the Chief Justice in *X (Re)* 2017 FC 1048 *(The BII Decision*) and the Reasons issued in 2018 FC 874 (*The BII Procedures Decision)*. (BII refers to Basic Identifying Information.) The Court questioned whether the

concerns noted and findings made by the Chief Justice in the *BII Decision* and the process described in the *BII Procedures Decision* should apply to this Application or whether the different context permits the decisions to be distinguished.

[2] The Court's questions, as amplified by the *amicus curiae* [the *amicus*] have been considered with the benefit of the submissions of the Attorney General of Canada [AGC] and of the *amicus*, the evidence of the affiant, [redacted], and the jurisprudence.

[3] In brief, I find that there are similarities between the issues considered and findings made in the *BII Decision* and *BII Procedures Decision* and the provisions at issue in this Application, namely Condition 3 and paragraph 5 (b) of the [redacted] Warrant. The principles set out by the Chief Justice in these two decisions are not in dispute and have provided guidance. However, there are distinctions that can be made, including with respect to the nature of the threat being investigated and its fluid nature, the continuing *nexus* between the threat being investigated and the privacy interests that may be implicated, and the extent of the intrusiveness into the privacy rights of the individuals affected.

[4] Following their written and oral submissions to the Court, the *amicus* and Counsel for the AGC continued to discuss their respective positions. As a result, CSIS proposes to amend paragraph 5 (b) and certain conditions of the [redacted] Warrant to ensure that the provisions at issue reflect both the underlying jurisprudence and the need for CSIS to execute the warranted powers to investigate [cyber threats] [redacted]

[5] I have concluded that Condition 3, as presently worded in the [redacted] Warrant in the context of [cyber threats] [redacted] at issue, is the appropriate way to ensure that the warrant is executed in accordance with the authority granted by the Court with respect to [investigative interests] [redacted] not specified at the time the warrant is issued, and that a fresh warrant application would not be required in this context. However, I also agree that the proposed amendments (more fully described below) provide added safeguards and should be implemented.

[6] I have also concluded that paragraph 5(b) is not an unlawful delegation of a judicial function in the context of [cyber threats] [redacted]. This context is sufficiently distinct from that in the *BII Decision*. Paragraph 5 (b) does raise similar concerns to those noted by the Chief Justice in the *BII Decision* because it delegates to the Director at CSIS the authority to obtain additional subscriber information based on the determination by a Chief at CSIS that comes to light after the Designated Judge has issued the warrant. Paragraph 5 (b) of the [redacted] warrant is currently not subject to Condition 3; in other words, there is no requirement to seek the authority of the Court to execute the power to obtain subscriber information from targets identified in the course of the investigation. Further consideration of whether paragraph 5(b) should be subject to Condition 3 may be advisable in some circumstances, in which case, the Designated Judge could impose such a condition. However, there are several differences between the subscriber information sought in reliance on paragraph 5 (b) in the [redacted] warrant context than in the context of the *BII Decision*, which distinguishes the findings in the *BII Decision*.

[7] I also agree that the proposed amendments to paragraph 5(b) and the related amendment to Condition 5 will better ensure that the powers of CSIS are appropriately narrowed.

[8] To better understand my conclusions and how the proposed amendments respond to residual concerns, I will describe the relevant background to this Application, the provisions at issue, the guidance from the *BII Decision* and *BII Procedures Decision*, how BII can be distinguished from subscriber information in the [redacted] warrant context, the positions of the *amicus* and the Attorney General, and the proposals which CSIS intends to adopt on a go-forward basis.

II. **The Provisions at Issue**

A. *Condition 3 of the* [redacted] *Warrant*

[9] Condition 3 states,

> Where, pursuant to paragraphs 1(c), 2(c), 3(a) (ii), 3(b) (ii) and 4(b), the Chief or his designate has identified a [redacted] [further investigative interest], for the purpose of executing this warrant, an application shall be brought to the Court, without delay, to seek authority to execute the warrant powers in respect of the identified [further investigative interests] [redacted]
> [Emphasis Added]

(Paragraphs 1(c), 2(c), 3 (a) (ii), 3 (b) (ii) and 4(b) refer to "any other [redacted]", "any other [redacted]" or "any other [redacted]" as applicable. Condition 3 requires CSIS to seek the Court's authorization to execute the interception or other

warranted powers with respect to the [identified further investigative interests] i.e., those that have not been set out in the warrant.)

[10] The question raised by the Court and *amicus* regarding Condition 3 is whether the process by which CSIS obtains further authorization to execute any of the initial warrant powers against new investigative interests is lawful.

[11] The *amicus'* initial position was that this is a new intrusion into the privacy of an individual and is, therefore, a new search, which must be authorized in the same manner as the initial warrant.

B. *Paragraph 5(b) of the* *Warrant*

[12] Paragraphs 5 (b), (c) and (d) state,

> 5. I authorize the Director and any employee of the Service acting under his authority to:
>
> […]
>
> (b) obtain subscriber information relating to any account where a Chief determines that the account was identified during the investigation of the threat to the security of Canada and the identity of the subscriber to the account will assist in the investigation of the threat to the security of Canada;
>
> (c) obtain the used to referenced in 5(b), and the it was used; and
>
> (d) obtain the used to it was used and the corresponding subscriber information.

[…]

[Emphasis Added]

These paragraphs delegate to the Director at CSIS the power to obtain subscriber information relating to [redacted] accounts that subsequently come to the attention of CSIS based on a determination made by a Chief.

[13] The *amicus* questioned whether such a delegation is lawful, noting that the determination of whether a search is reasonably justified is a judicial function. The *amicus* noted that in the *BII Decision*, the Chief Justice rejected a similar delegation to the Director to authorize collection of BII based on the identification by a Chief at CSIS. The *amicus* argued that paragraphs 5 (b), (c) and (d) of the [redacted] Warrant in the cyber threat context makes the same delegation, and in accordance with the *BII Decision* and the underlying jurisprudence, would be unlawful.

III. ***The BII Decision***

[14] In the *BII Decision* the Chief Justice addressed three related issues, one of which focussed on whether the Court can 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 determines that the account was identified during its investigation and that the BII will assist in its investigation.

[15] BII is described as consisting of the name and address of a subscriber to a communications account, [and the information relating to IP addresses in certain circumstances]

[redacted]

[16] In the overview, the Chief Justice noted at para 6:

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

[17] The Chief Justice explained that where the Court is not able to conduct 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 gaining access to their BII, CSIS must return to the Court for authorization each time it identifies additional telephone numbers or electronic identifiers in order to obtain the BII. CSIS would be required to establish the *nexus* between the number or identifier and the investigation (i.e., the threat) to establish that there are reasonable grounds to believe that CSIS requires the BII of the account to advance the investigation.

[18] With respect to whether the Court could authorize CSIS to obtain BII relating to other numbers or electronic identifiers that come to its attention in the course of an investigation based on the determination by a Chief at CSIS, the Chief Justice found that this was a judicial function that could not be delegated.

[19] At para 14 of the *BII Decision*, the Chief Justice added: "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 communication accounts will be the subject of requests to CSPs [Communications Service Providers] 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 interest of CSIS in obtaining the BII in question, this is a function that must be performed by the Court."

[20] The Chief Justice considered the jurisprudence regarding the search power and section 8 of the *Charter* and provided a detailed analysis which led to his findings.

[21] The Chief Justice elaborated, at paragraphs 91- 94, on the issue of the delegation to a Chief at CSIS. In particular, the Chief Justice noted at para 93:

> [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).

[22] The Chief Justice provided this summary at para 99:

> [99] In summary, the 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 maybe the subject of requests to CSP's 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.

[23] The *BII Decision* is relevant to the consideration of the lawfulness of Condition 3 and paragraph 5 (b) in the [redacted] warrant context.

IV. **The *BII Procedures Decision***

[24] In the subsequent *BII Procedures Decision*, at para 95, the Chief Justice addressed proposed provisions similar to Condition 3 of the [redacted] Warrant and set out the approach to be followed by CSIS on a go forward basis, which CSIS agreed would be adopted:

> [95] Based on representations made to the Court… 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 CSP's 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 the Court of the matters referred to in paragraphs 21(2) (a) and (b) of the Act. For greater certainty, these 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 identifiers] [redacted] 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's investigation into the 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 such application.

iii. In urgent situations where it is not possible to obtain the Minister's designation /approval or the Deputy Minister's confirmation of consultation, in writing, it will suffice if the Attorney General or her representatives (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.

[Emphasis Added]

[25] As an observation, the adoption of the approach set out in the *BII Procedures Decision* in the [redacted] Warrant in the context of [cyber threats] [redacted] would render Condition 3 meaningless.

V. **How does subscriber information in this Application ([redacted] Warrant) differ from BII?**

[26] In the *BII Decision*, the Court addressed the circumstance where the individual, once identified, would be a subject of investigation or may be in a position to assist in the investigation. As noted, the Chief Justice found, among other things, that the *nexus* between the individual and the investigation into the threat must be established. The Court must be satisfied that there are reasonable and probable grounds to believe that the individuals behind the telephone numbers and electronic identifiers either may be involved in the identified threat to the

security of Canada that CSIS is investigating or may be able to provide information to assist CSIS's investigation of the threat.

[27] As explained by the affiant, [redacted], in the [redacted] warrant context the target is the [redacted].

[28] [redacted] explained that subscriber information allows CSIS to find out [redacted]. He noted that in this context, CSIS is more interested in [redacted]. Although the identity of the [redacted] is needed, [redacted] The subscriber information is needed to [redacted]

[29] [redacted] explained that CSIS would first ask the [redacted]. CSIS would then approach the [redacted] and would seek the subscriber's consent to [redacted]. If no consent is provided, CSIS would seek a further warrant from this Court.

[30] Although the *amicus* submits that BII and subscriber information are basically the same, the Chief Justice described BII more broadly, as including the name and address of a subscriber to a communications account, [and the information relating to IP addresses in certain circumstances] [redacted]. The use of BII as considered in the *BII Decision* also differs from the use of subscriber information in the [redacted] warrant context.

VI. How does the initial warrant application made pursuant to sections 12 and 21 differ from the supplemental application contemplated by Condition 3?

A. *The Application*

[31] The application for the warrant at issue is typical of the current process. The application for the initial warrant included a detailed affidavit setting out how the warrant meets the statutory requirements of sections 12 and 21 to investigate [cyber threats] [redacted]

[32] The affidavit described the nature of the [cyber threat] [redacted], including what CSIS has learned about the methodology used and the characteristics of [redacted]. The affidavit also described how CSIS [redacted].

[33] The affidavit described the powers sought in the warrant and why these are necessary.

[34] The affidavit explained that the ability to obtain subscriber information of individuals contacting or interacting with threat actors assists in the investigation by identifying the threat actor, [redacted]. The affidavit explained that the power to obtain subscriber information corresponding to any [electronic identifiers] [redacted] will allow CSIS to identify the [redacted] and will allow CSIS to identify the victims of [redacted].

[35] Of note, the affidavit specifically addressed the need for Condition 3, which permits CSIS to seek authority from this Court, without delay, to execute the warranted powers (e.g. to intercept, obtain a copy of data, obtain information) in respect of newly identified [redacted] [investigative interests] identified during the life of the warrant.

[36] The affidavit included, among other exhibits: a description of [redacted], what CSIS intercepts and obtains, how CSIS minimizes the impact on privacy of Canadians; and, the specific [investigative interests] [redacted] for which CSIS is seeking the warranted powers at that time.

[37] The affidavit attested that the Deputy Minister of Public Safety and Emergency Preparedness [PSEPC] had been consulted and that the Minister of PSEPC had designated the affiant to make the application and has approved the application. The signed consultation and approval were attached as Exhibits.

B. *The Condition 3 "Supplemental" Application*

[38] Condition 3 contemplates that CSIS would make an application in writing, by way of a letter to the Court noting that it seeks to rely on Condition 3, providing a brief explanation and attaching a short affidavit and a draft Order identifying the newly identified [investigative interests] to be added to the Warrant previously issued. The affidavit references the application for the initial warrant and the affidavit filed in support of that application, which provided extensive details (as noted above).

[39] This process has not required an oral hearing, although nothing prohibits the Court from requesting a hearing if the Court has concerns or questions. Alternatively, the Court could request additional information in writing. The application in writing is not accompanied by a new record of consultation with the Deputy Minister or new approval of the Minister as this would entail delays which would undermine or preclude CSIS's ability to investigate [cyber threats].

[40] Although any Designated Judge could consider the supplemental application, and in doing so would review the warrant and the affidavit filed in support of the initial warrant application, where feasible, the same Designated Judge should consider the supplemental application which relies on Condition 3. The Designated Judge who heard the warrant application and granted the warrant would be familiar with the background information, including the *nexus* between the threat being investigated and the subscriber information being sought.

C. *The Application made in [redacted]; A Hybrid*

[41] An application to the Court pursuant to Condition 3 was made during the currency of the warrant seeking to add new [investigative interests] [redacted] and seeking authorization for the warrant powers to be executed with respect to the new [investigative interests] [redacted].

[42] I have characterized the [redacted] application as a hybrid because CSIS sought an oral hearing of the application, provided an affidavit describing how the [new investigative interests] [redacted] had been identified and explained why it was necessary for CSIS to query the information. In addition, the application included documents confirming that the Deputy Minister of PSEPC had been consulted and the Minister of PSEPC had approved the application to add new [redacted] [investigative interests] [redacted]. Counsel for the Attorney General noted that this was an unusual step which had been taken because of the questions posed by the Court regarding Condition 3 for which submissions of the AGC and *amicus* were pending.

[43] The supplemental application was granted following a hearing.

VII. **Is Condition 3 lawful, or is a fresh warrant application required to execute the warrant powers against additional [investigative interests]?**

A. *The Amicus' Position*

[44] The *amicus* submits that CSIS is required to seek a fresh warrant pursuant to section 21 to obtain authorization to engage in an intrusion against new [redacted] [investigative interests] [redacted]

[redacted] associated with [cyber threats] [redacted]. The *amicus* explains that additions requested by CSIS expand the number of individuals whose privacy interests would be engaged and intruded upon.

[45] The *amicus* submits that any intrusion requiring warrant powers requires judicial authorization, which in turn requires the judge to weigh the threat against the intrusion on the privacy of the investigative interest. In addition, the other statutory requirements for a warrant must be met: the Director, or an employee designated by the Minister, must believe, on reasonable grounds, that a warrant is required to enable the Service to investigate a threat to the security of Canada; the Director, or an employee designated by the Minister, must consult with the Deputy Minister regarding the application for a warrant; and, the Minister be made aware of the *particular* circumstances of the *specific* intrusion in order to determine whether to approve the application.

[46] The *amicus* characterizes Condition 3, as presently worded, as a blanket authorization to CSIS to seek judicial authority to conduct new intrusions without consideration of the specific circumstances that could justify the intrusion upon the privacy of individuals and without consultation with the Deputy Minister or approval of the Minister.

[47] The *amicus* submits that Condition 3 deprives the Minister of PSEPC of considering the factual *nexus* between the person whose privacy will be intruded upon and the threat.

[48] However, the *amicus* also acknowledges that in the context of [cyber threats] , the *nexus* between the threat and the new [investigative interests] is the same as that described in the initial warrant, where the same [investigative interests] are attributed, and that the privacy interests of the individuals affected by the warrants are the same.

B. *The AGC's Position*

[49] The AGC characterizes Condition 3 as a measure of control that applies at the time the warrant is executed with respect to the additional [investigative interests] , because it requires that CSIS return to the Court to seek authorization to execute the powers against those added.

[50] The AGC submits that Condition 3 remains the best approach to execute the warrant with respect to new [investigative interests] in the context of the investigation of [cyber threats] given the "fluid nature" of those activities. There is no need (as in the *BII Procedures Decision*) for a "fresh" application to be made or for a new Ministerial Approval or new Deputy Minister consultation. The initial warrant application includes the Deputy Minister consultation and Ministerial Approval which applies to the warrant and its conditions throughout the life of the warrant.

[51] The AGC explains that at the time Condition 3 is invoked, the threat is known, the methods which gave rise to identifying the additional [investigative interests] have been established, and the type of communication to be intercepted or information to be obtained is the same. The extent of the intrusion of privacy has been considered by the

Court at the time of the issuance of the initial Warrant and this remains the same for any additional [investigative interests]. The AGC submits that the basis upon which the Minister of PSEPC approved the application for the initial warrant remains unchanged.

[52] The same facts that CSIS would establish if required to make a new application to execute the warrant powers against new targets have already been established for the purpose of the issuance of the initial warrant.

C. *Condition 3 is a Lawful Condition*

[53] Condition 3 permits CSIS to seek authorization to execute the warranted powers against newly identified [investigative interests] without providing a new affidavit and without providing documents to show that the Deputy Minister of PSEPC has been consulted and that the Minister of PSEPC has approved the additions.

[54] Condition 3 ensures that the warrant is executed in accordance with the authority granted by the Court with respect to [further investigative interests] not specified at the time the warrant is issued. An application made to the Court pursuant to Condition 3 should not be characterized as a new application, rather as a supplemental application, which relies on the condition in the initial warrant (i.e. Condition 3) that operates for the duration of the warrant (which is not longer than one year). The Designated Judge who considers the supplemental application will have access to the application for the initial warrant and the affidavit(s) in support, the transcript of the hearing, the supplemental written application (which relies on Condition 3), and a shorter affidavit explaining why the newly identified [investigative

[redacted] should be added to the warranted powers. (As noted above, where feasible, it is preferable that the same Designated Judge consider the supplemental application.)

[55] The Designated Judge will consider the supplemental application and may issue the Order without an oral hearing (and without a new approval of the Minister of PSEPC or evidence of consultation with the Deputy Minister). However, if the Designated Judge is not satisfied that the Order should be made based on the written application or the supporting documents, the Judge could request an oral hearing and/or could request further documents.

[56] In the *BII Procedures Decision*, at para 95, the Chief Justice reiterated that where BII is sought from CSPs with respect to newly identified electronic identifiers, the correct approach is to bring a fresh application, with a fresh affidavit setting out, among other information, the *nexus* between the investigation and the identifiers, and a fresh designation and approval of the Minister of PSEPC and confirmation of consultation with the Deputy Minister of PSEPC. The Chief Justice explained that to satisfy the requirement for the *nexus*, the affiant should set out the reasonable and probable grounds for the belief that the individuals behind the identifiers may be involved in the threat or may be able to provide information to assist in the investigation into the threat.

[57] The Chief Justice emphasized that the Court must have an understanding of the *nexus* between the CSIS investigation and the "specific persons or class of persons" whose privacy rights would be engaged so that the Court can then assess whether the specific interests of those persons should give way to the interests of the state to obtain the information.

[58] The Application at issue- to execute warrant powers against newly identified targets in the [redacted] warrant context, relying on Condition 3- differs from the request for judicial authorization to obtain BII in the applications considered in the *BII Decision*. In the [redacted] warrant context, the threat is well established at the time of the initial warrant. The *nexus* between the [investigative interests] set out in the initial warrant as well as those identified in the course of the investigation and the threat being investigated is the same. In other words, the reasonable and probable grounds to believe that CSIS requires the subscriber information to investigate the threat remain the same for the newly identified targets.

[59] The extent of the intrusion into the privacy of the newly identified [investigative interests] is limited to identifying the [redacted]. The outcome of the balancing exercise (i.e., whether the specific privacy interests of the persons [redacted] should give way to the interests of the state to obtain the information) that would be required at the stage of the initial warrant application and at the time of the supplemental application pursuant to Condition 3 are not specifically known but would generally be the same. As explained by [redacted], CSIS does not seek information about the individual or their lifestyle, but only their identity for the purpose of determining [redacted]. Any further intrusions, [redacted], without consent, would require further authorization from the Court (i.e. a fresh warrant application).

[60] The concerns noted by the *amicus* regarding the protection of privacy arising from online anonymity, as recognized by the Supreme Court of Canada in *R v Spencer* 2014 SCC 43 [*Spencer*], at paras 47-48, do not arise. CSIS is not attempting to link a person's online activity with their lifestyle choices or with any other aspect of the individual's personal affairs, rather to [redacted].

[61] The supplemental application which relies on Condition 3 must be carefully considered and approved by the Court, but does not require a fresh warrant application and all that is entailed. The Designated Judge will consider whether CSIS has established the need to add the new [redacted] [investigative interests] [redacted] based on the information provided in the supplemental application with regard to all relevant information, including the initial warrant application.

[62] In this context, I find that a fresh approval by the Minister of PSEPC is not required to establish that the Minister is aware of the specific additions of [investigative interests]. Similarly, the proof of consultation with the Deputy Minister of PSEPC is not required.

[63] The Deputy Minister and Minister of PSEPC would have been aware at the time of the request for the initial warrant that Condition 3 would permit the warranted powers to be executed against others who come to the attention of CSIS in the course of the investigation over the duration of the warrant (which does not exceed one year) and that Condition 3 requires the Court to authorize the additions, or in the words of Counsel for the Attorney General, to exercise a measure of control.

[64] Although I find that Condition 3 of the [redacted] Warrant, as presently worded, is not unlawful, the proposal developed by CSIS and the *amicus* will provide an added safeguard that should be implemented. CSIS proposes to leave Condition 3 as is, and to amend Condition 4 to clarify that where the activity being investigated under the [redacted] warrant is [redacted], CSIS must bring a fresh application for a warrant. This new condition would address concerns about the *nexus* between the person(s) whose privacy rights would be engaged and the threat being investigated and would require the Minister to consider the particular circumstances of the search and the *nexus* to the identified threat. Where the activity relates to the threat described- i.e., where the *nexus* has already been established- there is no need for a fresh warrant.

[65] Condition 4 would be amended to add the wording in italics:

> Within 21 days of the date on which the Chief or his designate determines the [redacted], the Court shall be advised in writing, of the [redacted].
>
> *Should the* [redacted]*, a new application under section 21 of the CSIS Act shall be brought to the Court in respect of the* [redacted].

[66] The proposed amendment would clarify that CSIS cannot rely on Condition 3 when [redacted]. In such cases, a fresh application would be required in order to execute the powers sought. Any information obtained and used pursuant to Condition 3 in the very short intervening period prior to CSIS bringing a new application under section 21 can be considered to have been

lawfully obtained in exigent circumstances as long as it retroactively authorized by the Court as soon as possible.

VIII. **Is Paragraph 5(b) an unlawful delegation of a judicial function?**

A. *The Amicus' Submissions*

[67] The *amicus* notes that Section 8 of the Charter requires judicial pre-authorization for a search, and submits that this includes a search for subscriber information.

[68] The *amicus* notes that to comply with section 8 of the *Charter*, section 21 of the *CSIS Act* requires the Court to conduct an individualized assessment of the privacy of the person to be searched and to weigh that person's right to privacy against the state's interest in intruding upon their privacy. Section 21 of the *CSIS Act* provides that only a Designated Judge of this Court has the authority to authorize warranted searches. This judicial act cannot be delegated.

[69] The *amicus* points to the Supreme Court of Canada's decision in *Spencer*, which found that an individual has a reasonable expectation of privacy in their online anonymity, and that the authorities must obtain a warrant before obtaining subscriber information from a CSP. The *amicus* submits that the subscriber information sought by CSIS pursuant to paragraphs 5 (b), (c), and (d) would connect an individual subscriber to his or her real-world or online activity and would engage the anonymity aspect of privacy.

[70] The *amicus* views paragraphs 5 (b), (c) and (d) as an 'end-run' around the requirement for judicial pre-authorization because these provisions delegate the judicial function to determine whether the search is authorized to the CSIS Director.

[71] The *amicus* notes that in the *BII Decision*, at paras 91- 94, the Chief Justice rejected a similar delegation, finding that the CSIS Director or employee cannot decide if and when CSIS is justified in intruding into the privacy of an individual. Such decisions must be made by a Designated Judge.

[72] Although the Chief Justice noted, at para 77 of the *BII Decision*, that Justice Noël had previously granted a warrant delegating the authorization for the search of subscriber information (and related information) to a CSIS Regional Director General (or his designate) because of exigent circumstances, the Chief Justice was of the view that this delegation was subject to a condition which required CSIS to return to the Court for the authorization to execute the warranted powers (i.e., like Condition 3). The *amicus* notes that no such condition applies to paragraphs 5 (b), (c) and (d) and adds that no such condition applied in the example cited by the Chief Justice.

[73] The *amicus* submits that paragraph 5 (b) permits CSIS to obtain subscriber information, which is functionally the same as BII, of an individual whose privacy interests may have never been considered by the Court, i.e., the search has not been authorized by the Court. The *amicus* submits that a Designated Judge must balance the interests of the state against those of the

specific individual whose privacy interests are at stake. Where paragraph 5 (b) is relied on, this does not occur.

[74] Although the individuals whose subscriber information is sought may not be suspected of involvement in threat related activity, but are likely victims [redacted], the *amicus* submits that obtaining the subscriber's identity is nonetheless a search.

[75] The *amicus* further submits that the conditions in the warrant that provide that CSIS retain only threat related information are not sufficient protection of the privacy of the individual identified. The *amicus* notes that paragraph 5 (b) permits CSIS to authorize the search of added targets and that CSIS could retain this information and could share it with other agencies, including the police, without any review by the Court. The *amicus* adds that, as presently worded, paragraph 5 (b) and the current conditions permit information to be retained if it "will assist" in the investigation of an alleged contravention of <u>any</u> law of Canada (Condition 2). The *amicus* submits that this permits information to be retained by CSIS that may not be relevant to the specific cyber threat.

B. *The AGC's Position*

[76] The AGC submits that paragraph 5(b) does not require judicial pre- authorization to comply with section 8 of the *Charter* and therefore, it is not an unlawful delegation of a judicial function.

[77] The AGC acknowledges that in the *BII Decision*, the Chief Justice found that the determination by the CSIS Director or a Chief to seek BII from newly added identifiers would be an impermissible delegation of the judicial function, but argues that the *BII Decision* can be distinguished in several respects.

[78] The AGC submits that BII differs from obtaining subscriber information in the [cyber threat] context. BII is sought to identify an individual in relation to the investigation- i.e. either to get information about the investigation or because the individual is involved. In the [cyber threat] investigation context, subscriber information effectively constitutes the [redacted]. Subscriber information is sought to [redacted] in order to gain insight on the [redacted].

[79] The subscriber information does not reveal information about the subscriber's online activity or details of their lifestyle or choices or other personal affairs. As such, their privacy rights are not engaged or, to the extent that their privacy rights are engaged, the intrusion is minimal. The AGC emphasizes that without this minimal invasion of privacy, CSIS could not continue its essential investigations into cyber threats.

[80] The AGC notes that at the time of the initial warrant application, the Court considers whether the requirements of section 21 are met and whether the warrant should issue. The evidence provided at that time addresses, among other things, the nature of the threat, the threat activities, the conduct of the investigation and how the information gathered will be used. At the

hearing of the Application for the warrant, the Court must be satisfied that there is a *nexus* between the investigation and the persons or class of persons whose privacy rights would be engaged. It is at this stage that the Court balances the privacy of the subscribers (those identified in the warrant and those to be later/ subsequently identified) and considers whether the identified individuals' right should give way to the state's interest in obtaining the necessary information to investigate the threat.

[81] The AGC submits that, therefore, the determination by the Director and the Chief of [redacted] does not usurp a judicial function because the *nexus* has already been considered and determined to exist by the Designated Judge and the balancing of interests has already been conducted.

C. *Paragraph 5 (b) is not an unlawful delegation of a judicial function in the* [redacted] *warrant context*

[82] In the *BII Decision*, the Chief Justice addressed the issue of whether CSIS could prospectively be authorized to obtain BII in relation to communication accounts that may come to its attention in the course of the investigation where CSIS has not established the specific *nexus* between the accounts and the investigation. The Chief Justice found that it could not, highlighting, at paras 61-62, the need for an assessment of the context of each particular situation and the impact on the individual and the need to balance the interests of the state and the specific individual:

> 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* at 157,

> *Spencer* at para 36). 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 to be conducted is between the interests of the state and the interests of the specific individual whose privacy interests are at issue (*Hunter* at 159-60….) (other citations omitted).

[83] The Chief Justice acknowledged, at paras 64 and 65, that the name of the specific individual implicated is not likely known, but that other information can be provided to the Court regarding the reasonable and probable grounds relied on by CSIS to obtain the particular communication accounts.

[84] The Chief Justice also clarified, at para 62, that where the Court understands the *nexus*, the balancing can be conducted:

> [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 [i.e., at para 61] 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.

[85] Such is the case in the present context; the Court understands the *nexus* and has determined that there is a *nexus* between the individual(s) who are the subscribers and the threat being investigated at the time the [redacted] warrant is issued. That *nexus* remains the same over the duration of the warrant.

[86] Although the *amicus* argues that "class of persons" should not be interpreted to include those subscribers that come to the attention of CSIS in the conduct of the investigation, I am of the view that "class of persons" would capture this group in this context.

[87] As the *amicus* notes, the Chief Justice's comment at para 77 of the *BII Decision*, suggesting that the conditions of the warrant would require CSIS to return to Court before executing the warranted powers against newly identified targets, are not applicable in the present context. Condition 3 of the [redacted] Warrant does not apply to paragraphs 5(b), (c) and (d). CSIS is currently not required to seek authorization before obtaining subscriber information based on the Regional Director or his or her designates assessment of the need to do so. Where a the Designated Judge has concerns about the execution of warranted powers against newly identified targets, the Designated Judge could consider whether to impose Condition 3, or a condition similar to Condition 3. However, Condition 3 is not required as a general condition in order to render paragraph 5(b) lawful.

[88] The [redacted] warrant context is sufficiently different from the context which led to the Chief Justice's findings in the *BII Decision.* The *BII Decision* leaves room for the Court to take a different approach in the different context of the [redacted] warrant for cyber threats.

[89] Among the differences, as noted above, the Designated Judge has found that a *nexus* exists between the subscriber information sought and the threat at the time the warrant is issued. The same *nexus* exists for subscribers subsequently identified in the course of the investigation of the threat.

[90] In addition, the subscriber information obtained in reliance on paragraph 5 (b) is for the purpose of assisting CSIS to identify [redacted]. CSIS is not seeking details about the individual subscriber. The subscriber information is not used to gather intimate details of the person's lifestyle, personal choices or other personal affairs. The search is "not more than minimally intrusive", a distinction noted in the *BII Decision* at para 93.

[91] The nature and scope of the intrusion into the privacy of the, as yet, unknown subscriber is considered at the time the warrant is sought. The balancing of the privacy interests is conducted by the Designated Judge at that time. The balance remains the same with respect to subscribers identified in the course of the investigation of the threat. In these circumstances, the balancing conducted by the Designated Judge continues to apply because the subsequently identified subscribers are of the same nature (or same "class of persons") as those identified in the initial warrant with similar privacy interests.

IX. **The Proposal of the *Amicus* and CSIS**

[92] Although I have found, for the reasons noted above, that paragraph 5(b), as presently worded in the [redacted] warrant does not constitute an unlawful delegation of a judicial function, the amendments to paragraph 5 and the addition of Condition 5, as proposed by the *amicus* and CSIS, address concerns regarding the distinction between subscribers who are often victims of [redacted] and subscribers who could be targets of the investigation.

[93] The amended Paragraph 5 (b) would provide:

> I authorize the Director and any employee of the Service acting under his authority to:
>
> […]
>
> (b) obtain subscriber information relating to an [redacted] where the Chief has reasonable grounds to believe the [redacted] [Emphasis added]

[94] As amended, paragraph 5 (b) is narrower, more specific and better reflects the scenarios where subscriber information will be requested during the life of the warrant.

[95] This amendment would be complemented by a new Condition 5 which provides;

> Any information obtained pursuant to Paragraphs 5 (b) and (c) of this warrant shall be initially reported with the following notation: "A request made for subscriber information under paragraphs 5 (b) or (c) of the [redacted] Warrants is not an indication that the subscriber is engaged in threat- related activity."

[96] The AGC explains that the amendment to paragraph 5 (b) adds "reasonable grounds to believe" criteria for the determination by the Chief of [redacted] that the subscriber to a communications account would be either [redacted], as those terms are defined in the warrant. The AGC notes that the amendment to paragraph 5(b) would reflect the current practices as described by [redacted] and would address the concern noted by the *amicus* that the individuals who are identified when subscriber information is obtained are not generally engaged in threat related activities, and

therefore, any identifying information obtained should include an acknowledgement that they are not targets.

[97] In conclusion, the amendment to paragraph 5 (b), to narrow the power to obtain subscriber information, should be implemented along with the addition of new Condition 5 to require that the report on the information obtained indicate that the request for subscriber information does not signal that the subscriber is engaged in threat related activity. The new Condition 4, to clarify that CSIS cannot rely on Condition 3 where the activity is [redacted], should also be implemented.

[98] As noted above, Condition 3 does not currently refer to paragraph 5(b). As a result, the CSIS Director's authority to obtain subscriber information of newly identified [investigative interests] does not require that CSIS first seek the Court's authority to execute the warranted powers. There may be circumstances in the future where the Designated Judge will consider whether Condition 3 or a similar condition should be imposed with respect to paragraph 5(b).

"Catherine M. Kane"

Judge

FEDERAL COURT

SOLICITORS OF RECORD

DOCKET:	CONF-2-19
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] [CYBER THREATS] [redacted]
PLACE OF HEARING:	OTTAWA, ONTARIO
DATE OF HEARING:	JUNE 28, 2018 MAY 8, 2019
TOP SECRET REASONS:	KANE, J.
DATED:	OCTOBER 30, 2019

APPEARANCES:

Karla Unger Jessica Winbaum	FOR THE APPLICANT
Gordon Cameron	*AMICUS CURIAE*

SOLICITORS OF RECORD:

Attorney General of Canada Ottawa, Ontario	FOR THE APPLICANT (DEPARTMENT OF JUSTICE NATIONAL SECURITY LITIGATION AND ADVISORY GROUP)
Blakes Cassels & Graydon LLP Barristers and Solicitors Ottawa (Ontario)	AMICUS CURIAE