Federal Court  Cour fédérale

~~**TOP SECRET**~~

Date: 20210903

Docket: CSIS 17-19
CSIS 18-19
CSIS 19-19

Citation: 2021 FC 919

Ottawa, Ontario, September 3, 2021

PRESENT: The Honourable Mr. Justice Gleeson

BETWEEN:

IN THE MATTER OF AN APPLICATION BY […] FOR A 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 […]

BETWEEN:

IN THE MATTER OF AN APPLICATION BY […] FOR A 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 […]

BETWEEN:

IN THE MATTER OF AN APPLICATION BY […] FOR A 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 […]

ORDER AND REASONS

[On September 29, 2022, the Attorney General of Canada brought a motion pursuant to Rules 3, 55, 397 and 399 of the *Federal Courts Rules* SOR 98/106 seeking an Order varying the September 3, 2021 Order for the purpose of clarifying the circumstances in which the caveat at paragraph 43 is to be applied. The motion sought the following: to vary the wording of the caveat itself, to specify the Information Technology systems in which the caveat was required to be applied, and to specify that caveat is not required in those cases where a person is already known to the Service. By classified Order dated December 1, 2022 the Motion was granted. Paragraph 43 of this Public Order reflects the resulting amendment to the language of the caveat.]

I. Overview

[1] One of the early steps to be taken by the Canadian Security Intelligence Service [CSIS or the Service] in the investigation of threats to the security of Canada is the identification of those individuals who may be involved in threat-related activities. Obtaining the identifying information of the subscriber to a communication account (a telephone number or electronic identifier [electronic identifier(s)] discovered in the course of an investigation is one means of accomplishing this.

[2] The Service has previously sought and obtained judicial pre-authorization to collect what has been labelled Basic Identifying Information [BII] from Communications Service Providers [CSPs] to assist in identifying the subscriber to a communication account where the Service has demonstrated a *nexus* between an ongoing investigation and the specific account (*X (Re)*, 2017 FC 1048 at paras 3, 6 and 62 - 69 [*2017 BII Decision*] and (*X (Re)*, 2018 FC 874 at para 95 [*2018 BII Decision*], at para 95 [collectively the *BII Decisions*]. Understanding the *nexus* between the investigation and the account allows the Court to engage in an assessment of whether an individual subscriber's right to be secure against unreasonable search and seizure, pursuant to section 8 of the *Canadian Charter of Rights and Freedoms*, Part 1 of the *Constitution Act, 1982*,

being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [*Charter*], must give way to the State's interests in obtaining the BII (*2017 BII Decision* at paras 3, 6, 60 and 61).

[3] BII is a subset of subscriber information. It was defined in the warrants under consideration in the *BII decisions* as being limited to:

A. The name of a subscriber to an account;

B. The subscriber's address;

[certain other information related to the account] (*2017 BII Decision* at paras 2 and 32).

[4] The Service has found that in many instances the BII dataset is too limited to allow the successful identification of the users or owners of an identified communication account. To address this limitation, the Service brought three separate Applications for warrants pursuant to sections 12 and 21 of the *Canadian Security Intelligence Services Act*, RSC 1985, c C-23 [*CSIS Act*], seeking authorization to obtain a broader range of personal information from the CSPs. This broader set of information is labelled in the three Applications as Identifying Information [II]. The definition of II is set out below at paragraph 12.

[5] The three Applications relate to different aspects of the Service's investigation of the Islamist Terrorism threat. The II relating to […] identified communications accounts was sought to assist in identifying the account subscribers, non-warranted techniques having been exhausted.

[6] The Applications were granted in part. A two phase approach to the II warrants was adopted to limit the information the Service was authorized to obtain to that demonstrated as necessary to further the ongoing Service investigations while minimizing the intrusiveness of the authorized search.

[7] In Phase 1 the Service was authorized to collect a subset of the II sought [Phase 1 II]. Phase 1 II was broader than BII but excluded potentially more intrusive subscriber information and the identifying information of other individuals potentially connected to an identified communications account. In the event that the Phase 1 II did not enable the Service to identify an account subscriber Phase 2 recognized that the Service might pursue a supplementary application, seeking authority to collect the II not included in the Phase 1 authorization.

[8] These reasons detail the manner in which the Applications were addressed and the basis for having adopted a two phase approach to the Applications for authority to collect II. The reasons also consider the need for additional warrant conditions relating to the retention and use of II by the Service.

II. Background

A. *Why Three Applications?*

[9] In bringing these Applications the Service continued to refine its approach to seeking BII warrants, or in these instances, II warrants. Instead of seeking warrants supported by a general affidavit addressing the threat as a whole, Islamist terrorism in this instance, the Service proceeded with three separate and distinct Applications, [CSIS 17-19, CSIS 18-19 and CSIS

19-19, each related to a different aspect of the Service's investigation of the Islamist Terrorism threat].

[10] The Service's refined approach was intended to facilitate the presentation of supporting evidence and to better demonstrate whether the Service has established the required *nexus* between the communication accounts of interest and the ongoing Service investigation.

[11] In CSIS 19-19, [...]

B. *What is Identifying Information [II]*

[12] II was defined in each of the three Applications as follows: [The BII plus certain other information related to the account to assist in the identification of the user or owner of the account].

[13] II, as defined above, unquestionably encompasses a broader suite of personal information than BII (see para 4 above) and includes information that is more detailed and potentially more intrusive than that considered in the *BII Decisions*. It also captures information connected to […]. For example, II includes the information of [certain other information related to the account].

C. *The Proceedings*

[14] An *in camera ex parte* hearing was held where the primary affiant in each of the three Applications, […] provided *viva voce* evidence. […] evidence details how each category of

II for which authorization was being sought would be of assistance to the Service in the conduct of its investigation, and in particular assist in identifying the subscribers to the identified communications account.

[15] The II warrants placed before me did not include what had been Condition 1 in previous BII warrants. Condition 1 of the BII warrants required that the Service, where relying on [certain other information related to the account, take certain measures. This requirement] is now reflected in the II definition (see subparagraph 12(K) above). The Attorney General was of the view that this rendered Condition 1 of the BII warrant superfluous. I agreed.

[16] On the completion of the hearing I reserved my decision on each of the Applications and appointed an *amicus curiae* to assist in assessing whether the broader definition of II raised questions for consideration beyond those addressed by Chief Justice Paul Crampton in the *BII decisions*.

[17] In bringing the Applications, the Attorney General identified two issues:

A. Do the applications for warrants meet the statutory requirements set out in the *CSIS Act*; and

B. Is the information requested limited to what is necessary to reveal identity and not permit more serious intrusions into privacy?

[18] The second issue engaged considerations that warranted the appointment of the *amicus curiae*. In appointing Mr. Cameron, I restated the second issue, as follows:

> Does the broadened definition of II raise issues or engage considerations that differ from or go beyond those addressed in the BII decisions?

[19] Upon completion of his documentary review, Mr. Cameron identified issues relating to: (1) the collection of II, and (2) the retention and use of II.

[20] In addressing the retention and use issue, the *amicus* took the position that were the Court to authorize the collection of II, the Court should also consider the need for additional warrant conditions. The Attorney General was of the view that further conditions were not required and that in any event the types of conditions suggested presented operational and technical obstacles for the Service. Further affidavit evidence was filed and the affiants, […] and […] were examined.

[21] I address both the collection and retention issues raised by the *amicus* in turn, beginning with the collection issue.

III. Authorizing the Collection of II

[22] The Attorney General submitted that the broader definition of II as set out in the three Applications did not impede the Court's ability to balance the competing interests between the State's need for the information and the individual privacy interests as detailed in the *BII Decisions*. The *nexus* needed to satisfy constitutional requirements for authorizing the intrusive

activity was established in the evidence, as was the need for the Service to obtain the more intrusive II.

[23] The *amicus* was of the view that section 21 of the *CSIS Act* reflects, as a general principle, that as a search becomes more intrusive, the burden on the Attorney General to justify the search should also increase proportionally. Applying this principle to the three II Applications, the *amicus* argued the Court should approach and adopt the BII standard of a *nexus* cautiously because BII was determined to be minimally intrusive information.

[24] In advancing this view, Mr. Cameron noted that the broader definition of II would result in the collection of personal information that was more intrusive than that considered in the BII decision. II captured more detailed subscriber information (for example it includes […] and authorized the collection […].

[25] Establishing a mere *nexus* between the investigation and a communication account may not, Mr. Cameron submitted, be sufficient to authorize the collection of more intrusive II. He noted for example that a court might not be satisfied that the evidence establishes on reasonable grounds that all categories of II are initially required to enable the Service to investigate the threat or that all categories of II are of importance with respect to the threat (*CSIS Act* paras 21(2)(a) and 21(2)(b)). It will therefore, he submitted, often be an issue as to whether all categories of II are to be authorized, particularly where all the Service can initially establish in its Application for II is the possibility that less intrusive information may be insufficient to identify an account subscriber.

[26] In response to these submissions the AG and the *amicus* jointly proposed, and I agreed, that the II Applications should proceed in two phases. In Phase 1, I considered the Applications on the basis of a narrowed definition of II that excluded personal information [of a certain type] or personal information that was clearly more intrusive than that considered in the *BII Decisions*.

[27] II was defined in Phase 1 as follows:

[The BII plus a subset of II that is limited to account subscriber and is less intrusive than the total of II.]

[28] The *amicus* acknowledged the narrowed scope of Phase 1 II but noted it is nonetheless potentially more intrusive than the identifying information contemplated in the *BII Decisions*. He submitted the Court should therefore be mindful that reliance on a mere *nexus* between the investigation and a communications account might be insufficient grounds for the issuance of a Phase 1 II warrant.

[29] While I do not disagree with the *amicus'* position that the more intrusive a search the greater the burden on the Attorney General to justify the intrusion, it is important that I make two points. First, although the Phase 1 definition of II as set out above engages more categories of information than BII, Phase 1 II, as defined, is not different in kind from BII. I am therefore of the view that it does not capture information that is necessarily more intrusive than BII.

[30] Secondly, I do not read the *2017 BII Decision* as standing for the general proposition that a mere *nexus* between a Service investigation and a communication account will always justify the issuance of a BII warrant. Instead, satisfaction of the *nexus* requirement allows the Court to meaningfully consider the interests of a specific individual or class of individuals whose privacy interests are engaged while taking into account: (1) the individual's subjective expectation of privacy; (2) that the Service's powers to investigate threats to the security of Canada be strictly controlled; and (3) that the totality of the circumstances are to be taken into account (*2017 BII decision* at para 63). This remains the case where authorization to collect II is sought.

[31] Mindful of, and after having considered these factors, I was satisfied, on reasonable grounds, of the existence of a threat to the security of Canada, that a *nexus* had been established between each of the identified communication accounts for which II had been sought, and the Service investigation. I was further satisfied, on reasonable grounds, that the evidence established Phase 1 II, as defined at paragraph 27 and relating to the identified communications accounts, was needed to enable the Service to further its investigation. The Phase 1 II warrants […] the Service had sought in CSIS 19-19 were granted.

[32] Supplementary applications, seeking Phase 2 II, were not brought by the Attorney General.

[33] As noted above, the *amicus* also identified concerns relating to Service retention of, and access to, lawfully collected II. I remained seized of the Applications for the purpose of determining if as a result of the issues identified by the *amicus* further terms or conditions

governing retention and use of II would be advisable in the public interest. I turn to that issue now.

IV. Conditions on Retention and Use of II

[34] In considering II, as defined in the three Applications (see para 12), the *amicus* took the position that even if the intake of II was demonstrated as necessary to further a Service investigation, some of the II lawfully collected might prove, upon examination, not to be necessary or even relevant to the investigation. Collection authorization should not necessarily justify the indefinite retention and unlimited or uncaveated access to information that proves to be unnecessary or irrelevant to an investigation, particularly if the information relates to […].

[35] The *amicus* submits that when authorizing a broader intake of II the Court should be satisfied that the Service has addressed questions relating to the retention of, and access to, information that on examination proves to be unnecessary or irrelevant. If not satisfied that the Service information management practices are sufficient in this regard, the Court may specify terms and conditions in the warrant (*CSIS Act* para 21(4) (f)). Conditions might, for example, require destruction of unnecessary or irrelevant information or, where retention is required for some demonstrated purpose, require the information be flagged and/or sequestered as a means of managing retention and access. A broad intake authorization combined with unrestricted retention and access invites over-intrusive data retention, the *amicus* argues.

[36] The *amicus* further submits that even though Phase 1 II limits collection to account subscriber information, this does not exclude the possibility that an individual account subscriber

may prove to have virtually no connection to the threat investigation. For example the subscriber may have […]. The *amicus* submits that if there is no involvement in threat related activity, one might presume the II is unnecessary or irrelevant to the Service investigation. While this information was authorized for collection and therefore satisfies the statutory retention standard at section 12 of the *CSIS Act* (strictly necessary) as that provision was interpreted and applied in *X (Re)*, 2016 FC 1105, the *amicus* submits that the Court may nonetheless impose conditions on use and retention on the basis that the information was obtained pursuant to the Court's authority.

[37] The Attorney General acknowledges that warrant conditions may be imposed by an authorizing judge in the public interest. However, the Attorney General notes that the exercise of judicial discretion in this regard should be informed by sections 12 and 21 of the *CSIS Act* and the limits imposed by section 8 of the *Charter* as it has been judicially interpreted. The Attorney General submits that the minimization of intrusive activity is not a mandatory requirement where warranted collection is authorized but also acknowledges that conditions are frequently imposed for the purpose of minimizing the intrusive nature of warranted activities, particularly where third parties may be affected by the use of warranted powers or authorities.

[38] The Attorney General submits that information collected through a Phase 1 II authorization is limited to account subscribers and is narrowly targeted. The information is necessary to allow the Service to identify users and assess the nature of the users' relationship to the threat being investigated and that the limitation to retention at section 12 of the *CSIS Act* - the

"strictly necessary standard" – is a sufficient basis to retain the information. Additional conditions are not required (*X (Re)*, 2016 FC 1105).

[39] The Attorney General argues that the II of the subscriber to an account linked to threat-related activity who, after examination, is determined to be an individual not involved in threat-related activity, is nonetheless information that is relevant and necessary to the Service investigation. In support of this position, the Attorney General relies on the operational evidence of […].

[40] In her operational affidavit, […] addresses the importance of retaining and being able to access II even where it is believed after consideration of the II and any further investigation that the person is not engaged in threat-related activity. This information, she states, allows the Service to close the investigative loop, its retention avoids incomplete or fragmented operational reporting that might hinder investigations or create intelligence gaps. […] evidence is that the information is also retained for the following reasons:

i. [future use in the same or other investigations; and]
ii. […]
iii. […]
iv. […]
v. Accountability, reviewability and other corporate considerations.

[41] The evidence of […] addressed the Service's technical challenges and limitations in implementing Conditions on the retention and use of II.

[42] Having carefully considered the evidence, and in particular the evidence provided by […] in her operational affidavit, I am of the view that Phase 1 II, as defined at paragraph 27 above, is information that is relevant and necessary to the Service's Islamist terrorism investigation, even where the Service does not have reasonable grounds to believe that the identified individual was or is engaged in threat-related activity. I also note that Condition 1 of the warrants provides that any information other than the authorized II obtained in the execution of the warrants shall be destroyed. As such, I am not convinced that additional conditions are needed or are appropriate in respect of the retention and use of lawfully collected Phase 1 II. I reach this conclusion with two qualifications.

[43] First, the Attorney General and the *amicus* have agreed upon a caveat that may be attached to II upon collection and maintained so long as the Service does not have reasonable grounds to believe that the identified individual was or is engaged in threat-related activity. The proposed and agreed upon caveat reads as follows:

> The information in this report was collected for preliminary investigative reasons as there were reasonable grounds to suspect that ~~the~~ a selector associated with [*cite the Identifying Information in this report or the name of the person*] was or is used to engage in threat-related activity. As of ~~the date of this report~~ [*insert date of assessment*] the Service does not have reasonable grounds to suspect that the person identified in this report was or is engaged in threat-related activity. Unless the Service acquires such grounds, this caveat must be repeated in any future report in which the identifying information in this report is repeated and in any intelligence disclosed to foreign or domestic partners ~~disclosure of the identifying information outside of the Service~~.

[44] The caveat places the II of individuals not identified as being engaged in threat-related activity in its proper context. The caveat also provides this notice to anyone accessing the II or

any reporting that includes the II. The technical evidence of […] was to the effect that the caveat may be attached to newly collected or existing information.

[45] I am satisfied that the proposed caveat is appropriate in this instance. The caveat shall be applied, where applicable, to the Phase 1 II that the issued warrants have authorized the Service to collect and shall also be attached to any subsequent reporting that includes the applicable II. I acknowledge that the circumstances of Phase 1 II collection may well differ in future applications and those circumstances may indicate the above-noted caveat is unnecessary.

[46] Second, my conclusion that the Phase 1 II as defined in the Applications is information that is relevant and necessary to a Service investigation and that additional conditions relating to use and retention are not warranted should not be read as extending to include the broader II that would be captured in a Phase 2 Application. In returning to the Court seeking authorization to collect Phase 2 II, the Service should be prepared to address the issues canvassed in these reasons, including whether some or all of the information sought in a Phase 2 II Application should be subjected to conditions on retention and use.

ORDER

THE COURT ORDERS that:

1. The caveat at paragraph 43 of these reasons shall be attached to the Phase 1 Identifying Information and any reporting that includes the Phase 1 Identifying Information collected under the Authority of the warrants issued in CSIS 17-19, CSIS 18-19 and CSIS 19-19 [...] where the Service does not have reasonable grounds to suspect that the person identified was or is engaged in threat-related activity.

2. This Order and Reasons shall be reviewed jointly by the *amicus curiae* and counsel for the Attorney General with a view to making a joint recommendation to the Court regarding redactions to the version of the Order and Reasons that will be made public. The Court shall be provided with a timeline for the submission of redaction recommendations within thirty (30) days of the date of this Order.

"Patrick Gleeson"
Judge

FEDERAL COURT

SOLICITORS OF RECORD

DOCKET:	CSIS 17-19 / CSIS 18-19 / CSIS 19-19
STYLE OF CAUSE:	IN THE MATTER OF AN APPLICATION BY [redacted] FOR A 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 [redacted] IN THE MATTER OF AN APPLICATION BY [redacted] FOR A 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 [redacted] IN THE MATTER OF AN APPLICATION BY [redacted] FOR A 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 [redacted]
PLACE OF HEARINGS:	OTTAWA, ONTARIO
DATES OF HEARINGS:	SEPTEMBER 24, 2019 FEBRUARY 17, 2020
ORDER AND REASONS:	GLEESON J.
DATED:	SEPTEMBER 3, 2021

APPEARANCES:

Penny Brady	FOR THE APPLICANT
Isabelle MacKay	THE ATTORNEY GENERAL OF CANADA

Gordon Cameron	*AMICUS CURIAE*

SOLICITORS OF RECORD:

The Attorney General of Canada	FOR THE APPLICANT
Gordon Cameron	*AMICUS CURIAE*