National Security and Intelligence Review Agency

Office de surveillance des activités en matière de sécurité nationale et de renseignement

TOP SECRET // CEO

REVIEW OF CSIS'S USE OF [redacted]A GEOLOCATION DATA COLLECTION TOOL (NSIRA STUDY 2018-05)

s.15(1)(d)(ii)

Contents

s.15(1)(d)(ii)

I AUTHORITIES

This review began under the authority of the Security Intelligence Review Committee (SIRC) as articulated in subsection 38(1) of the *Canadian Security Intelligence Service's (CSIS Act)*, which provided SIRC the mandate to review CSIS's operations in the performance of its duties and functions.

During the course of the review, Bill C-59 – *An Act Respecting National Security Matters* – received Royal Assent on June 21, 2019. Part 1 of Bill C-59 enacted the *National Security and Intelligence Review Agency Act* (NSIRA Act), which came into force by order of the Governor in Council on July 12, 2019. The *NSIRA Act* repeals the provisions of the *CSIS Act* that established and governed SIRC and establishes in its place the National Security and Intelligence Review Agency (NSIRA). The *NSIRA Act* sets out the composition, mandate and powers of NSIRA and amends the *CSIS Act*, and other Acts, in order to transfer certain powers, duties and functions to NSIRA.

This review continued under the authority described in subsections 8(1)(a) and 8(3) of the *NSIRA Act* to review any activity carried out by CSIS and to make any finding and recommendation that NSIRA considers appropriate.

II INTRODUCTION

In its review function, NSIRA expects CSIS's activities to be lawful and comply with ministerial direction. This review focused on CSIS's non-warranted collection of geolocation information and is part of NSIRA's ongoing interest in CSIS's collection and exploitation of both warranted and unwarranted data. Past reviews have assessed CSIS's warranted collection and retention of metadata and CSIS's unwarranted collection and exploitation of bulk personal datasets. This is NSIRA's first dedicated look at CSIS's collection of geolocation data.

The review takes place in the context of Federal Court decisions, most particularly the IMSI decision of September 27, 2017, that impact on CSIS's collection, use and retention of data, including geolocation data. The IMSI decision found that, though CSIS's authority under section 12 does authorize it to obtain geolocation information for which there is a low expectation of privacy, anything beyond that, such as geolocating an individual, would require a warrant.

It is worth noting that the scope of the review was broader at the outset and was intended to include a more comprehensive examination of the collection of different types of geolocation information, both warranted and unwarranted. Although the scope was reduced in the course of the review, NSIRA will be mindful of this for future reviews.

III OBJECTIVES

The objective of this review is to assess whether CSIS's collection of unwarranted geolocation

information used by CSIS in support of its operations is compliant with applicable sources of law, including the *Canadian Charter of Rights and Freedoms* (*Charter*) and the *CSIS Act*, as well as ministerial direction and operational policy. A related objective is to determine whether CSIS has sufficient safeguards in the form of formal procedures and policies to ensure that it is able to comply with its legal obligations amid a period of rapid change in technology and a correspondingly fluid legal environment.

s.15(1)(d)(ii)
s.16(1)(b)

IV SCOPE AND METHODOLOGY

The scope and direction of the review was identified through a preliminary investigation of available documentation and a briefing with the [redacted] Further, NSIRA requested that CSIS identify all activities undertaken by the [redacted] that may result in geographic information collected against non-warranted targets within the review period. This information was used as a foundation to request specific documents from CSIS.

NSIRA examined all documents provided by CSIS and sought, retrieved and reviewed documents through CSIS's various computer and email systems to ensure a clear record of activity. Documents reviewed included: [redacted] taskings from the regions, responses to these taskings, briefing notes, planning documents, legal assessments and internal correspondence.

To conduct a compliance assessment of CSIS's use of geolocation information, NSIRA chose to conduct an in-depth case study of [redacted] geolocation information. NSIRA reviewed all instances when [redacted] was used by CSIS during the period under review. As this review consists of a single case study, NSIRA is mindful of generalizing the findings and conclusions to other types of geolocation data.

The core review period for this study was from January 1, 2017 to June 30, 2018, although NSIRA examined documentation that fell outside this period in order to provide a complete assessment of relevant issues.

V CRITERIA

Legal and Ministerial Requirements

NSIRA expects CSIS to conduct its activities in accordance with relevant sources of law, including the *CSIS Act*, the *Charter*, the *Privacy Act*, and case law. NSIRA also expects CSIS to conduct its activities in accordance with ministerial direction.

Most relevant in this review given the subject matter was an analysis of the *Charter*, which, in

section 8, provides everyone with the right to be secure against unreasonable search and seizure. In this case, at issue was whether the use of [redacted] to collect information about an individual's location information constitutes a search for the purposes of section 8 such that a warrant would be required.

Policies and Procedures

s.15(1)(d)(ii)
s.16(1)(b)

NSIRA's expectation was that there would be policies and procedures in place to guide the collection, use and retention of data from [redacted] despite its uniqueness, and that those policies and procedures would support compliance with CSIS's legal obligations, including the *Charter*, as well as its obligations stemming from ministerial direction.

For reference, the relevant policies that pertain to the collection of information [redacted] are:

- [redacted] In principle, this allows collection of this nature on a very broad cross-section of individuals;
- The collection of [redacted] policies, including the DDO Memorandum of 2015 that requests the establishment of [redacted] as the National Policy Centre for [redacted] Additionally, there is the procedure on [redacted] that allows [redacted] to conduct [redacted] defined as a non-warranted collection tool or technique, against a [redacted]

VI BACKGROUND

The Investigative Technique - [redacted]

[redacted]

[1] CSIS Procedures: [redacted]
[2] CSIS Procedure: [redacted]

from users across the world.

[redacted] contains three months of data. The information is not available in real-time; however, there is a delay of only 24-48 hours between the collection of the [redacted] and it becoming available in [redacted]

s.15(1)(d)(ii)
s.16(1)(b)

[redacted]

See Annex A for an example of the use of [redacted] against a CSIS target.

A chronology of CSIS's use of [redacted]

s.15(1)(d)(ii)
s.16(1)(b)

a. From introduction to the beginning of the pilot: July 2015 – January 2018

[redacted]

[redacted] echoed those same governance-related issues; specifically, it questioned whether there were legal issues associated with [redacted] that needed to be addressed prior to the trial period. [redacted] asked for "the rules of engagement so that we can plan accordingly and get the most of this evaluation." [redacted] further noted that, although the data seemed "wonderful….there must be some legal/governance rules that apply to this when in the hands of a government agency."[6] These questions were raised in an email to both [redacted] and the [redacted]

[3] See timeline provided in response to SIRC question.
[4] 8 Sept 2015 - [redacted]
[5] Email, June 28, 2017, "FW [redacted]
[6] Email, September 27, 2017 [redacted]

[redacted] Nevertheless, by September 2017 [redacted] was anticipating an evaluation of [redacted] that would involve using [redacted] for a trial period of two months with a limited [redacted]

[redacted] convened a meeting in October with [redacted] The objective of the meeting was to prepare for a [redacted] evaluation and, for that purpose, "to make decisions on a few details to ensure compliance with legal and policy."[7]

s.15(1)(d)(ii)
s.16(1)(b)

The questions to be covered in the agenda were:

1) Does existing [redacted] policy cover the use of [redacted] or does the policy need to be adapted?
2) Is the information contained in [redacted] subject to a reasonable expectation of privacy?
3) Is there anything else that needs to be considered before CSIS can use [redacted]? For example, additional [redacted] procedures or tests?

According to a written summary of discussions[8] circulated by [redacted] following the meeting, it was agreed that [redacted] would be compliant with collection under the [redacted] which allows [redacted] to "research and use open information" in support of investigations. It was further decided that the use of [redacted] would align with [redacted] policies[9] as it would constitute threat related queries [redacted] and would be used only with the [redacted] authorities in place.[10] Finally, it was assessed that the [redacted] data ingested would meet the "strictly necessary" threshold for collection and retention as set out in the *CSIS Act* as it would be based on a specific threat.

[redacted]

Following the meeting, approval was granted for the trial use of [redacted] by Deputy Chief

[7] Email, October 18, 2017, "meeting summary [redacted]
[8] Email, October 18, 2017, "meeting summary [redacted]
[9] In particular, Memorandum to DDO from Chief [redacted]

[redacted]

[12] CSIS response to SIRC memo, November 15, 2018

[redacted][13]. Documentation of the approval consists of an email from the Deputy Chief to [redacted] and [redacted] with the understanding that, [redacted]

s.15(1)(d)(ii)
s.16(1)(b)

b. CSIS's trial period –March 2018 – July 2018

CSIS began its pilot of [redacted] on January 14, 2018. It was initially to be for two months; but because of technical issues at the beginning that delayed its full use, and due to [redacted]

During that time, [redacted] was tasked a total of approximately [redacted] times, resulting in [redacted] operational messages.[14] As noted, efforts were made by [redacted] to ensure that its use of [redacted] was compliant with CSIS's [redacted] policies on collection [redacted] as well as the *CSIS Act* provision that collection and retention be done only to the extent that is "strictly necessary."

[redacted] completed its evaluation of [redacted] by the end of April 2018. [redacted]

The first version of a briefing note to gain approval for the [redacted] was drafted jointly by [redacted] and [redacted] in April 2018.[16] The briefing note stated that the pilot for [redacted] was "conducted under [redacted] authorities and an assessment of the [redacted] deemed them compliant with current operational policies." The briefing note also [redacted] one was a restricted amount of information that would meet the strictly necessary threshold; and the other was a situation in which [redacted] in which case it would be [redacted]

A subsequent version of the briefing note was prepared, also jointly by [redacted][8] This one was dated May 15, 2018 and was sent to the Director General of [redacted] In contrast to the first version of the briefing note, this one had the dual purpose of obtaining a legal opinion and [redacted] This version was ultimately sent to the DG

[13] Email, September 29, 2017, [redacted]
[14] Response to SIRC memo, October 25, 2018 [redacted]
[16] Briefing Note, "Subject/Sujet: [redacted]
[redacted] Briefing Note, "Subject/Sujet: [redacted]

[redacted] and also included that [redacted] had been assessed as compliant with [redacted] authorities, following discussions with CSIS's External Review and Compliance (ERC), [redacted] as well as informally with a representative of the DLS. The briefing note stated that "[redacted] fall within existing authorities and directives" and, further, that "although [redacted] has assessed that [redacted] a formal legal opinion has not yet been conducted and suggest this briefing note be used as a mechanism to obtain one."

NSIRA inquired as to the substance of the ERC and DLS discussions, as well as documentation of those meetings. NSIRA was advised that the ERC compliance officer embedded within [redacted] was aware of [redacted] which was presented at a town hall, but that it was not discussed with her beyond that.[19] NSIRA asked for documentation to substantiate the DLS discussions but none was provided.[20]

c. Legal advice: July 2018 – February 2019

s.15(1)(d)(ii)
s.16(1)(b)
s.23

Following the May briefing note, on July 20th, the DG [redacted]

By July 31, preliminary legal advice was received:

[redacted]

A formal legal opinion was provided on December 7, 2018[23] that called into question CSIS's use of [redacted] without a warrant except in very narrow circumstances, [redacted]

[19] CSIS response to SIRC question, October 14, 2018
[20] SIRC memo to CSIS, October 31, 2018
[21] Email from DG [redacted] to DLS, July 20, 2018, Subject "FW: [redacted]
[22] Email, July 31, 2017, "RE: ADV – [redacted]
[23] Legal Memorandum, December 7, 2018, [redacted]

A further legal opinion was requested by CSIS to determine whether [redacted] The resulting legal opinion, dated February 19, 2019, [redacted] Accordingly, section 8 of the *Charter* would not be engaged in this narrow circumstance.

Based in part on the February 2019 legal opinion, CSIS subsequently took the decision to [redacted] It is NSIRA's understanding that, presently, [redacted] is being used only in very specific circumstances and according to the guidelines set out in the legal opinions.

s.15(1)(d)(ii)
s.16(1)(b)
s.23

VII FINDINGS

Finding no. 1 Compliance with the CSIS Act and the Charter

NSIRA finds that there was a risk that CSIS breached section 8 of the *Charter* during the trial period in which it used [redacted] without a warrant.

DLS was asked to provide a legal opinion to CSIS on this investigative technique; in particular, to address the question of the "legal risk of using [redacted] (i) with respect to Canadians or persons in Canada; and (ii) human sources and employees, with their informed consent". CSIS was advised in a Legal Memorandum dated December 7, 2018 that:

[redacted]

NSIRA's own review of the file, which is meant to provide the Committee with independent legal advice, supports DLS's opinion in that regard. In particular, NSIRA believes that the use of [redacted] constitutes a search for the purpose of section 8 of the *Charter*. In drawing this conclusion, NSIRA observes that it is very unlikely that a court would find that section 12 of *CSIS Act* was sufficient legal authority to render warrantless use of [redacted] "reasonable" for the purposes of section 8 of the *Charter*. Accordingly, CSIS would be required to obtain a warrant pursuant to

[24] Legal Memorandum, [redacted] December 7, 2018

section 21 of the *CSIS Act* for such searches. Of note, NSIRA's legal analysis was based on the same set of facts as DLS used for its opinion.

In reaching this conclusion, NSIRA interprets section 12 of the *CSIS Act* as only providing authority for collection activities of minimal intrusiveness. In that regard, NSIRA concurs with the DLS opinion that, [redacted]

At the time of writing, CSIS is pursuing options for how [redacted] may be used under the authority of a warrant in the future.

s.15(1)(d)(ii)
s.16(1)(b)
s.23

NSIRA recommends that CSIS review its use of [redacted] to date and make a determination as to which of the operational reports generated through the use of [redacted] were in breach of section 8 of the *Charter*. These operational reports and/ or any documents related to those results should be purged from its systems.

Findings no. 2 Governance related to piloting [redacted]

NSIRA finds that there was no policy centre clearly responsible for the use of the data contained in [redacted]

NSIRA asked about the policies and procedures that guided the decision to authorize the trial period, as well as which unit within the [redacted] branch would have been responsible for assessing and authorizing the use of [redacted] As described above, the record suggests there were three discrete units involved in the [redacted] for the trial period.

[redacted] was involved in the [redacted] As the policy centre with respect to the [redacted] the role and mandate of [redacted] is to coordinate, manage and [redacted] In this capacity, [redacted] would have been responsible for assessing [redacted] for privacy impacts, among other things, had [redacted] been assessed as a [redacted] However, [redacted] was not [redacted] but rather, as [redacted] Therefore, [redacted] did not officially assess [redacted] That said, the briefing note of May 15, 2018, clearly indicates that [redacted] assesses that the use of [redacted] fall within existing authorities and directives."[25] Given the lack of a formal record, NSIRA was unable to

[25] Briefing Note, "Subject/Sujet: [redacted] May 15, 2018

assess the content of, or the rationale for, this assessment.

[redacted] is the unit responsible for providing operational support for [redacted] intelligence through the use of covert [redacted] and it was to [redacted] that the first demonstration of [redacted] was given. [redacted] authorities were eventually identified as those under which [redacted] would operate. However [redacted] was not the primary user of [redacted] Neither did it participate in the formal evaluation of the data contained in [redacted]

Responsibility for developing a means of formally evaluating [redacted] fell to the [redacted] given its expertise in geolocation information. However, [redacted] does not generally collect data, but is merely the user of data provided to it. As such, [redacted] did not, nor was it directed to, conduct a thorough preliminary evaluation to determine whether there were legal or other issues that needed to be addressed, even at the pilot stage. Nevertheless, [redacted] prepared, on its own initiative, a formal document to guide its evaluation of [redacted] during the trial period. NSIRA also notes that [redacted] followed existing policy in using [redacted] only in instances when a valid targeting authority was in place.

s.15(1)(d)(ii)
s.16(1)(b)

NSIRA was not provided any formal documentation on the decision to authorize the pilot period. The record of decision to pilot [redacted] consisted of an email, which contained the following:

> I don't see any reason not to start an evaluation – [redacted] In addition, [redacted] are not provided until after we can determine that they are "strictly necessary" and of relevance to the investigation – just [redacted] until we find something of relevance.[26]

Ultimately, NSIRA was unable to identify which of the three policy areas within [redacted] should have had, according to existing policies and procedures, responsibility for the assessment of [redacted]

Finding no. 3 Record of decision

NSIRA finds that the record of approval to pilot [redacted] consisted of an email and that this email was not "put-away" as part of the official record, as it should have been.

As noted, the closest thing to a record of decision to pilot [redacted] was an email from a Deputy Chief of [redacted] the full text of which is cited above.

NSIRA notes that this email was not "put-away" as is should have been given that it represents, *de facto*, the approval for acquiring [redacted] for the purposes of evaluation and is required for robust records management and for accountability purposes. Instead, it was saved on a

[26] Email, September 29, 2017, [redacted]

"personal" drive and only produced as part of the review process.

Findings no. 4-5 Assessment of risk in the case of

NSIRA finds that there are no developed policies or procedures around the assessment and handling of new and emerging collection technologies, such that a formal evaluation of the legal risks of using would have been required.

NSIRA finds that CSIS overlooked multiple indicators that using might raise legal issues.

Ministerial Direction requires that the risk of operational activities be assessed across four pillars (operational, political, foreign policy and legal). In particular, the Direction states that CSIS should "consider its own level of experience and novelty of the operational activity in assessing risk".[27]

NSIRA was told that there is no formal process for the evaluation of risk in cases like given that it was assessed as [28] This is consistent with NSIRA's reading of the relevant policies, cited earlier, pertaining to of which require an assessment of legal risk prior to the use of for collection purposes.

It was suggested to NSIRA that it would not have been possible to conduct a thorough assessment of before the pilot based on the reasoning that a risk assessment is only possible with full [30] NSIRA accepts in principle that there are situations when it would be difficult to appreciate the legal risks until such time and fully evaluated. Notwithstanding the difficulties, it is the responsibility of CSIS to mitigate these risks to the extent possible.

In this case, moreover, NSIRA notes that there were indications of a need for caution with respect to the in the period before the trial was even begun, including the IMSI

[27] Ministerial Direction on Operations and Accountability, 2015
[28] CSIS response to SIRC memo, January 31, 2019
[29] CSIS response to SIRC memo, January 31, 2019
[30] Briefing with April 11, 2019

decision of the Federal Court, which found that geolocating an individual would require a warrant.

Internally, there were multiple indications to the effect that there may be reason for particular attention, including:

- two emails sent prior to the pilot, one by [redacted] on June 28, 2017, and the other by [redacted] September 27, 2017, both containing legal and governance questions;
- the meeting convened by [redacted] for the purpose of discussing whether there existed a reasonable expectation of privacy in the [redacted] data;
- the examples provided by [redacted][31] and
- the evaluation of [redacted] in April 2018, which indicated that there were privacy concerns with this tool given its ability to generate [redacted] and to [redacted]

s.15(1)(d)(ii)
s.16(1)(b)

There were other indications of a need for caution. [redacted]

[redacted]

[31] See, for example, [redacted]
[32] See, for example, [redacted]

[34] Email of May 28, 2018, "FW [redacted]

Despite these signs, no formal action was taken to assess the question of legal risk until the briefing note in May 2018 requested a formal legal opinion.

s.15(1)(d)(ii)
s.16(1)(b)

NSIRA recommends that policy be developed or amended as appropriate that would require a documented risk assessment, including legal risks, in situations like [redacted] when information collected through new and emerging technologies may contain information in respect of which there may be a reasonable expectation of privacy. If not [redacted] NSIRA further recommends that a policy centre for this type of [redacted] collection be clearly identified.

Conclusion:

At the outset, [redacted] was characterized as making use of [redacted] This is made clear from the approval email. [redacted] would consider, it is not clear that the data exploited through [redacted] represents genuinely [redacted] at least as defined in plain language, as was asserted.

Assessing [redacted] in this way was not without its consequences in that it appears to have justified the lack of a more thorough legal assessment. This assumption proved to be problematic; the consequence was that CSIS placed itself at risk of having violated the *Charter*.

Throughout this review, NSIRA has been mindful of the length of time it took for CSIS to obtain the final legal opinion, which was requested in July but finalized only in December, a full five months later.

NSIRA is aware that there have been discussions within [redacted] on the need to have ongoing legal support. In particular, [redacted] has requested the establishment of a policy and legal operating envelope to ensure that policy and legal questions related to data exploitation are properly covered, including a resource from DLS who would provide ongoing, even weekly, legal assistance.[35] NSIRA understands that this request was made in part due to the difficulties associated with obtaining legal advice on an as needed basis. NSIRA has been advised that [redacted] request to have weekly legal support has not yet been actioned.

The combination of an expanding scope in the type, volume and sources of data collected by CSIS and a fluid legal situation makes this an area of persistent high legal risk. CSIS has publicly affirmed that the concept of a reasonable expectation of privacy is evolving over time and committed to ensuring that CSIS's approach to a reasonable expectation of privacy "is kept consistent".[36]

---

[35] Email, July 4, 2018, "FW DLS assistance request"
[36] Geddes comment before the Standing Committee on National Security and Defence (SECU), February 13, 2019

NSIRA is of the view that, in this environment, legal support to [redacted] is essential to operate at an acceptable level of risk. NSIRA expects CSIS and the Department of Justice (DOJ) to demonstrate institutional leadership that would allow responsible decision-making in an environment of uncertainty by making available legal support to [redacted] as required on a priority basis.

s.15(1)(d)(ii)

ANNEX A: The Case of [redacted]

The case of [redacted] offers a good illustration of the potential of [redacted] as an investigative tool. [redacted]

[redacted][37] At the time this information was collected, CSIS was in the process of preparing an affidavit to seek warrant powers on [redacted] NSIRA reviewed the affidavit that was provided to the [redacted] to assess whether information from [redacted] had been used in support of the warrant application and found that no [redacted] information had been included.

s.13(1)(a)
s.15(1)(d)(ii)
s.16(1)(a)(iii)
s.16(1)(b)
s.19(1)

[37] [redacted]