



TOP SECRET

Date: 20170927

Docket: CONF-2-17

Citation: 2017 FC 1047

Ottawa, Ontario, September 27, 2017

PRESENT: THE CHIEF JUSTICE

BETWEEN:

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

and

**IN THE MATTER OF ISLAMIST
TERRORISM AND [REDACTED]**

PUBLIC JUDGMENT AND REASONS

I.	Introduction.....	3
II.	Background.....	6
III.	This Proceeding	10
IV.	Preliminary Issue Regarding the Openness of the Hearing on the Legal Arguments	14
V.	CSS technology.....	21
VI.	CSIS’s Policy Regarding the Collection and Retention of Electronic Identifiers	29

VII.	Assessment of Legal Submissions	31
A.	The Radiocommunication Act	31
B.	The Criminal Code.....	36
C.	Section 8 of the Charter	39
(1)	Legal principles.....	39
(a)	What Constitutes a Search or Seizure?	40
(b)	What Constitutes an Unreasonable Search or Seizure?	46
(2)	Application of the Legal Principles to the Facts of this Application.....	49
(a)	Did CSIS’s Use of CSS Technology Constitute a “Search”?	49
(i)	The Subject Matter of the Intrusive Activity	50
(ii)	Individuals’ Interest in the Subject Matter.....	53
(iii)	Do Individuals Have a Subjective Expectation of Privacy in the Subject Matter?	53
(iv)	If So, Are Such Expectations Objectively Reasonable?	54
	The Nature of the Privacy Interest at Stake	54
	The Circumstances in which IMSI and IMEI Identifiers Are Obtained.....	55
	The Manner and Place of the Capture of IMSI and IMEI Identifiers.....	55
	Whether the IMSI/IMEI Identifiers have been Abandoned or Disclosed to One or More Third Parties	57
	The Extent to which the Search Technique is Intrusive in Relation to the Identified Privacy Interest	59
	The Relevant Statutory and Contractual Framework.....	60
	Is the Use of CSS Technology Objectively Unreasonable?.....	68
	Conclusion Regarding the Objective Reasonableness of Individuals’ Subjective Expectations of Privacy in Relation to the IMSI and IMEI Identifiers of their Mobile Devices.....	69
(v)	Conclusion Regarding Whether the Capture of IMSI and IMEI Identifiers Constitutes a “Search.”	71
(b)	Is CSIS’s Interception of IMSI and IMEI Numbers Unreasonable?	72
(i)	Was the “Search” Authorized by Law?	73
(ii)	Is Section 12 of the Act a Reasonable Law?.....	77
	The Nature and Purpose of Section 12	78
	The Degree of Intrusiveness Authorized by Section 12	82
	The Extent to Which the Act Provides for Judicial Supervision	83
	The Presence of Other “Checks and Balances” or Accountability Measures.....	87
	Conclusion Regarding the Reasonableness of Section 12	89
(iii)	Was the Manner in Which the Search was Carried Out Unreasonable?	91
(iv)	Conclusion regarding the reasonableness of CSIS’s use of CSS technology	94
VIII.	Conclusion	95
	APPENDIX I	100
	APPENDIX II	101
	APPENDIX III	103

I. Introduction

[1] In a free and democratic society, it can be expected that citizens will not want the identifying characteristics of their mobile telephones to be surreptitiously obtained by anyone, including the Canadian Security Intelligence Service [CSIS], for the purpose of assisting to build a profile about them.

[2] However, unless it is unlawful for CSIS to engage in such activity, it is free to do so within the parameters established by its enabling legislation and the *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [the *Charter*]. The question to be decided in this case is whether the activity in which CSIS engaged to obtain such information from the mobile devices of a known subject of investigation, ██████████ was in fact unlawful. That activity was conducted without a warrant and involved CSIS's use of a cellular-site simulator [CSS] to capture the identifying characteristics of his mobile devices.

[3] Those identifying characteristics consisted of the International Mobile Subscriber Identity [IMSI] and International Mobile Equipment Identity [IMEI] numbers that were emitted by ██████████ mobile devices when they attempted to communicate with the cellular network of his telecommunications service providers [TSP]. The IMSI number identified the country in which ██████████ cellular account is located, the network code of his TSP, and the unique subscriber identifying number given to him by the TSP. The IMEI identified the make, model and unique serial number of his mobile devices.

[4] In my view, CSIS's use of a CSS without a warrant, and solely to obtain the identifying characteristics of [REDACTED] mobile devices, was not unlawful. This is in part because of a number of measures that were taken to ensure that the activity was minimally intrusive. So long as similar measures are followed by CSIS in the future, its CSS operations would also be lawful. In other words, they would not contravene the *Radiocommunication Act*, RSC 1985, c R-2, the *Criminal Code*, RSC 1985, c C-46, or the *Charter*.

[5] Generally speaking, the measures adopted by CSIS in carrying out CSS operations should strictly limit its intrusion on the privacy rights of the subjects of its investigations. In addition, these measures should ensure that CSIS does not capture the contents of any communications or any of the contents stored on, or available through, anyone's mobile device(s). They should also ensure that the incidentally captured information pertaining to the mobile devices of third parties is quickly destroyed and is not subject to any analysis whatsoever, once it has been confirmed that those devices are not the mobile device(s) used by the subject of investigation

[REDACTED] Furthermore, CSS technology should not be used to geo-locate anyone without a warrant.

[6] CSIS's use of a CSS against [REDACTED] constituted a "search" within the meaning of section 8 of the Charter. This is because [REDACTED] had a reasonable expectation of privacy in respect of the information that CSIS was in a position to begin to gather about him, or about which it was able to make informed inferences, upon gaining access to the IMSI and IMEI numbers of his mobile devices. In brief, those numbers assisted CSIS to begin building a profile on [REDACTED] including by potentially helping CSIS to determine his [REDACTED] [contacts] [REDACTED] and

communication patterns” with the aid of information already available to CSIS. To the extent that this enabled CSIS to begin to gain an understanding of, or to make reasoned inferences about, certain aspects of [REDACTED] core biographic personal information, it engaged his rights under s. 8 of the *Charter*.

[7] Nevertheless, the search was not “unreasonable,” because it was narrowly targeted, highly accurate and minimally intrusive. The CSS operations conducted by CSIS were even more minimally intrusive with respect to the information that was incidentally captured from the wireless devices of third parties, because that information was quickly destroyed and was not subject to any analysis whatsoever, after it was determined that the information did not pertain to [REDACTED] wireless devices.

[8] More generally, the evidence in this proceeding establishes that the CSS technology used by CSIS does not permit it to identify the individual whose mobile devices are targeted by the CSS operation, or to gain access to billing or other intrusive information. Indeed, the identity of targets of CSIS’s CSS operations, as well as their location and other information, typically is already known at the time such operations are conducted. Where CSIS requires detailed billing or subscriber information from a TSP, it will require a warrant. This is because of the more highly intrusive nature of such information, which can include a listing of all calls made during a billing period, the duration of those calls, and the locations of the parties to those calls.

[9] Agents of the state who are responsible for the safety and security of the general public may engage in minimally intrusive activities without violating section 8 of the *Charter* so long as

those activities are authorized by law, the law is reasonable, and the activity is carried out in a reasonable fashion. Such minimally intrusive activities can include the physical surveillance of people in public, and even the monitoring of the level of heat emanating from their homes. In this case, CSIS's use of CSS technology was authorized by section 12 of the *Canadian Security Intelligence Service Act*, RSC 1985, c C-23 [Act], section 12 is a reasonable law, and CSIS's search was conducted in a reasonable manner.

II. Background

[10] This is the first proceeding in which CSIS has explicitly sought the Court's views regarding its use of CSS technology to obtain information or intelligence in the course of an investigation, without a warrant.

[11] CSIS has used CSS technology for that purpose for several years. However, prior to February 10, 2016, the Court was unaware of this fact. On that date, CSIS provided the Court with a copy of the classified report of the Security Intelligence Review Committee [SIRC], entitled, *SIRC Review 2014-03—Review of CSIS's use of Metadata*. Among other things, that report referred to two case studies. The first was entitled *The Use of Metadata by the Operational Data Analysis Centre (ODAC)* and ultimately led to a decision by my colleague, Justice Simon Noël, concerning CSIS's program of collection and retention of such information (*X (Re)*, 2016 FC 1105 [*X (Re)*]). The second case study was entitled *The Service's Collection of International Mobile Subscriber Identity (IMSI) Data*, and provided a brief overview of the history of CSIS's use of CSS technology. In brief, after getting introduced to the technology

[15] Shortly after having had an opportunity to review SIRC's above-mentioned report, Justice Mosley again inquired about the use of CSS technology. The affiant in that hearing ██████████ testified that the technology had been used in the investigation that led to that application for warrants, and explained how the technology had been used. The affiant undertook to confirm that data from the mobile devices of third parties which is collected at the time of a CSS operation is destroyed by CSIS. That confirmation ultimately was provided on ██████████ and again by a senior employee of CSIS, ██████████ during the evidentiary hearing in this application.

[16] A similar inquiry was made by Justice Mosley, and a similar response was provided by another affiant, during the hearing of another application ██████████

[17] At a subsequent case management meeting that I co-presided with Justice Noël on ██████████ Justice Noël inquired about the "Stingray" technology, how it operates, and whether it was being used under this Court's warrants.¹ In response to Justice Noël's request, the Deputy Director Operations [DDO] of CSIS, Mr. Jeff Yaworski, undertook to obtain the relevant details and to provide them to the Court. It was only as a result of information subsequently provided by CSIS that the Court began to gain a more fulsome appreciation of the nature and extent of CSIS's use of CSS technology.

[18] On ██████████ counsel to CSIS confirmed in a letter to the Court that there were no other instances, apart from those mentioned above, in which references were made to CSS or

¹ Justice Noël is the Coordinator of the Court's Designated Proceedings Unit.

similar technology, in exchanges between the Court and CSIS or its counsel. At the end of that letter, the Court was informed that [REDACTED]

[REDACTED]

[REDACTED] This was the first time that the Court had been informed that CSIS was using CSS or similar technology pursuant to its warrants.

[19] [REDACTED]

[REDACTED]

[REDACTED]

[20] On [REDACTED] Justice Noël directed CSIS and the Attorney General “to provide information and evidence regarding the nature, scope, usage and minimization of the investigative technique called Stingray.” Justice Noël’s Direction added that “[t]he Court requires the information and evidence in order to fully and clearly understand the investigative technique; and, to assess whether [REDACTED] or any other warrant provides lawful authority for the technique.” Ultimately, CSIS decided to provide that information and evidence in the context of this proceeding.

III. This Proceeding

[21] In this proceeding, CSIS sought a number of warrants from the Court pursuant to sections 12 and 21 of the Act to permit it to continue to investigate the activities of [REDACTED] in connection with Islamist terrorism. As explained below, I granted those warrants with two amendments, for the period commencing on [REDACTED] and ending on [REDACTED]

[22] [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[23] The IMSI and IMEI numbers that were obtained from [REDACTED] wireless devices in [REDACTED] assisted CSIS to execute interception powers that this Court authorized in [REDACTED] by ensuring that those powers were exercised against the wireless devices described in this Court's warrants.

[24] In support of its application for warrants in this proceeding, CSIS relied on two affidavits, provided by [REDACTED] Affidavit] and [REDACTED] Affidavit]. In addition, CSIS and the *Amici* submitted a number of documents, including responses to undertakings given to me during the proceeding, that were marked as exhibits.

[25] [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[26] With two exceptions, the operative language of the warrants granted in this proceeding was identical to the language of the warrants that had previously been granted by Justice [REDACTED] in respect of [REDACTED] and that had been scheduled to expire on [REDACTED]. The first exception was that I included language which prohibits the use of CSS [REDACTED] in paragraph [REDACTED] Warrant. That prohibition has been included in several other warrants since the Court learned that CSIS had been relying on paragraph [REDACTED] in using CSS [REDACTED] against targets of the Court's warrants. In including that prohibition, I made it clear to CSIS and the Attorney General that this amendment to the warrant should not be taken as any pronouncement by the Court with respect to the legality of the CSS technology, whether or not used pursuant to a warrant, as these remained "live" issues in this application [REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]

[27] The second amendment that I made to the warrant powers sought in this proceeding was to delete the requested authorization to obtain [REDACTED]

[REDACTED] That amendment was made after I determined that the evidence adduced by CSIS did not establish reasonable grounds to believe that [REDACTED]

[REDACTED]

[28] On [REDACTED] at the end of the evidentiary hearing in this proceeding, I granted the warrants sought by CSIS, with the two amendments described above. I did so after satisfying myself that, among other things, CSIS had established that there were reasonable grounds to believe that [REDACTED] activities constitute a threat to the security of Canada, as defined in paragraph 2(c) of the Act, and that CSIS required the warrants to investigate that threat.

[29] In making my decision to grant those warrants, I relied on the evidence provided by [REDACTED] which included considerable information obtained in the course of CSIS's

investigation of Islamist terrorism as well as more specific information concerning [REDACTED]. That information was obtained through various methods of investigation, including physical surveillance and warranted intercepts involving [REDACTED]

[REDACTED] Additional information was also collected from human sources, interviews, open information, government agencies in Canada and foreign agencies that are investigating Islamist terrorism. I did not rely on the very limited information

that was obtained by CSIS using CSS technology against ██████ without a warrant. That information was obtained through the use of the technology during a two-day period, and simply consisted of the attribution of three devices to ██████ namely, ██████ ██████ According to one of the affiants in this proceeding, that information has now been destroyed. For greater certainty, I also did not rely on any information that was derived from the IMSI and IMEI numbers obtained through CSIS's use of CSS technology, including communications over any of those devices that were subsequently intercepted by CSIS.

[30] In issuing the most recent warrants against ██████ I made it clear that I would remain seized of this application in order to (i) take notice of the amendments to this Court's warrant templates that are ultimately made as a result of the decision that Justice Simon Noël issued on October 4, 2016, in *X (Re)*, above, (ii) make corresponding amendments to the warrants that I have provisionally issued in this proceeding, and (iii) make any further amendments to those warrants that I consider appropriate, after having had an opportunity to consider the legal submissions made in this proceeding.

[31] As an aside, and for completeness, it is relevant to note that the Attorney General confirmed in a letter dated ██████ that the only instances in which the language of ██████ was relied on were ██████ geo-location CSS operations. The Attorney General added that CSIS did not rely on any warrants issued by this Court to conduct any of its other past CSS operations, because it does not consider that it requires a warrant to capture IMSI and IMEI numbers for the purposes of attributing a device to a subject of investigation.

[32] This proceeding was organized as an *en banc* hearing because it involves the first application to the Court in which CSIS has (i) explicitly stated that it had resorted to CSS technology in the course of investigating the activities of its subject of investigation, (ii) made submissions on the lawfulness of its use of the technique in that investigation, and (iii) provided evidence regarding its use of that technology. I considered it appropriate to convene the other designated judges of the Court to join me on the bench, so that they would have the benefit of the evidence provided by [REDACTED] including on cross-examination by the *Amici*. I also considered it to be important that they have the benefit of responses provided by [REDACTED] to questions that any of them, or I, might pose. This should assist each of the designated judges of the Court in future applications involving CSS technology, and may reduce the need for similar evidence in such applications.

[33] Notwithstanding the presence of other designated judges of this Court in this proceeding, I assured CSIS and representatives of the Attorney General at the outset of the hearing that was held on [REDACTED] that my judicial independence would not thereby be compromised in any way. I, and I alone, have decided the issues that have been raised in this application.

[34] Given the importance of the legal issues raised in this application, the Court retained Mr. Gordon Cameron and Mr. Owen Rees to act as *amici curiae*.

IV. Preliminary Issue Regarding the Openness of the Hearing on the Legal Arguments

[35] During the evidentiary hearing on [REDACTED] I learned that there is more information in the public domain regarding CSS technology and its use by law enforcement

agencies than I had previously appreciated. With that in mind, and having regard to the recent significant increase in public interest concerning the oversight of CSIS's activities by the Court, I invited the Attorney General's views as to whether it was necessary for the hearing of legal arguments concerning the CSS technology to be held *in camera*.

[36] Counsel to the Attorney General undertook to seek instructions and get back to the Court on this matter. However, she observed that CSIS likely would be reluctant to participate in a public hearing on this issue, given that its use of CSS technology had never been publicly acknowledged.

[37] Subsequently, in a letter dated [REDACTED] the Attorney General took the position that a public hearing of the legal submissions in this hearing would not be suitable. In brief, the Attorney General submitted that such a public hearing would be contrary to section 27 of the Act and could cause serious injury to Canada's national security interests. Among other things, the Attorney General maintained that a public hearing would adversely impact [REDACTED]

[REDACTED]

[REDACTED]

Instead of a public hearing, the Attorney General proposed that a public decision be issued, subject to appropriate redactions.

[38] Section 27 of the Act states:

Canadian Security Intelligence Service Act, RSC 1985, c C-23

Loi sur le Service canadien du renseignement de sécurité, LRC (1985), ch C-23

27. An application under section 21, 21.1 or 23 for a warrant, an application under section 22 or 22.1 for the renewal of a warrant or an application for an order under section 22.3 shall be held in private in accordance with regulations made under section 28. (Emphasis added)

27. Une demande de mandat faite en vertu des articles 21, 21.1 ou 23, de renouvellement de mandat faite en vertu des articles 22 ou 22.1 ou d'ordonnance présentée au titre de l'article 22.3 est entendue à huis clos en conformité avec les règlements d'application de l'article 28. (Je souligne)

[39] In support of its position that a public hearing of the legal arguments in this proceeding would be contrary to the explicit terms of section 27, the Attorney General relied on the following passage from Justice Noël's decision in *Canadian Security Intelligence Service Act (Re)*, 2008 FC 300, at para 34:

[34] Section 27 provides that applications for warrant "shall be heard in private" ("huis clos" in French). "Private" is defined as "confidential; secret" in Brian A. Garner, *Black's Law Dictionary*, 8th ed. (St-Paul: Thomson West 2004), s.v. "private" In Hubert Reid, *Dictionnaire de droit québécois et canadien*, (Montréal, Wilson & Lafleur, 1994), s.v. "huis clos", the expression "huis clos" is described as being "une exception au principe de la publicité des débats, qui consiste à interdire au public l'accès à la salle d'audience". Again, the main aims of the privacy of applications for a warrant are to preserve the secrecy of sensitive information in general and to ensure the execution of warrant [*sic*]. The interested person(s) (targets) must not be present or aware of the warrant application; otherwise its purpose would become academic. The public should not have access to the information because it is related to national security and because of the effectiveness of the CSIS depends on the secrecy of its methods

and operations. Finally, third party information is often transmitted under the caveat that it would not be released. If warrants were debated in public, sensitive information would likely be released advertently or inadvertently. It would prevent the CSIS from being informed about threats to Canada's security, would render useless the investigation, would be dangerous to human sources involved and could endanger Canada's relationship with allied countries.

[40] However, the Attorney General failed to note that Justice Noël proceeded to observe, at paragraph 46 of his decision, that “issues that are ‘collateral’ to a warrant application, such as jurisdictional issues, could be heard in open courts in some circumstances.” In this regard, Justice Noël emphasized that “each case turns on its facts keeping in mind the clear wording of section 27 of the [Act] and the necessary balance between national security and fundamental rights” (para 47). Ultimately, Justice Noël concluded that the issues of law and of fact in the particular case that was before him were so intertwined that the jurisdiction issue that had been raised could not be dealt with in public.

[41] In the present proceeding, it was not initially apparent to me that the factual and legal issues were similarly intertwined. However, it subsequently transpired that the factual evidence adduced was critical to the findings I ultimately made in respect of the issue of whether CSIS's use of CSS technology constituted a search, as well as the issue of whether that search was “unreasonable,” within the meaning of section 8 of the *Charter*.

[42] The Attorney General's stated reasons for opposing a public hearing were significantly undermined by two important developments that occurred between the time of the evidentiary hearing and the hearing of the parties' legal submissions. The first of those developments was that

the Minister was reported to have publicly confirmed the use of CSS technology by CSIS and the RCMP, but only “within the four corners of the law” (“RCMP, CSIS launch investigations into phone spying on Parliament Hill after CBC story,” *CBC News* (April 4, 2017) online: < www.cbc.ca >.) The Attorney General confirmed this fact in a letter to the Court dated April 5, 2017, yet continued to maintain that “the hearing [of the legal] submissions concerning the Service’s use of CSS must continue to be held in camera in order to comply with section 27 of the [Act] and to avoid serious injury to national security interests.”

[43] The second important intervening development consisted of a CBC news article, published the day before the hearing of the legal submissions in this proceeding, in which CSIS was reported to have “confirmed that it has used the cellphone identification and tracking technology in recent years, both with and without a warrant” (“Spies’ use of cellphone surveillance technology suspended in January, pending review,” *CBC News* (May 3, 2017) online: < www.cbc.ca >.)

[44] In light of that reported confirmation by CSIS of its use of CSS technology, the *Amici* sent a short letter to the Court suggesting that the circumstances were such that the hearing of the legal submissions in this proceeding should be made open to the public. While recognizing the requirement in section 27 that warrant applications be heard in private, they observed that certain statements made by the Supreme Court of Canada in *Canada (Citizenship and Immigration) v Harkat*, 2014 SCC 37 [*Harkat*], “would support a decision by the Court to make the legal argument on the Service’s use of cell site simulators open to the public.” At paragraph 25 of that decision, the Supreme Court observed that the issues in that case did “not turn on confidential

information and could have been debated fully in public without any serious risk of disclosure, supplemented where necessary by brief closed written submissions and by the closed record.”

The Court proceeded to add, at para 26, that the content of the closed part of the hearing in that case did not assist the Court in deciding the issues before it, and “served only to foster an appearance of opacity of these proceedings, which runs contrary to the fundamental principles of transparency and accountability.” The *Amici* did not address the differences between the case that was before the Supreme Court and the application that is before this Court in the current proceeding.

[45] In response to the *Amici*'s suggestion, the Attorney General sent a short letter to the Court later that day in which she agreed to discuss the possibility of holding a public hearing.

However, the Attorney General noted that an adjournment might be required in order to identify which elements could be heard in a public hearing and which would require consideration *in camera*. The Attorney General also “urge [d] consideration of section 27 of the [Act].”

[46] At the outset of the hearing of the legal arguments in this application the following morning, the *Amici* once again suggested that the Court adjourn the hearing to permit them to work with the Attorney General to devise a means to have at least part of the oral legal submissions made in a public forum.

[47] However, given the last-minute nature of the *Amici*'s suggestion, and in the absence of additional submissions from the *Amici* and the Attorney General as to how a public hearing

could occur given the express language of section 27, I decided to proceed with the hearing, as previously scheduled.

[48] In reaching that decision, I was cognizant of the decision in *Ruby v Canada (Solicitor General)*, 2002 SCC 75, at paras 57–58, where the Supreme Court of Canada observed that it was not open to the parties, even on consent, to bypass the mandatory *in camera* requirement set forth in paragraph 51(2)(a) of the *Privacy Act*, RSC 1985, c P-21. The Court added that, constitutional issues aside, it was also not open to a judge to conduct an open hearing, even if only in respect of legal issues, in direct contradiction of the statute, regardless of the proposal put forth by the parties. (For constitutional reasons, the Court then proceeded to “read down” certain provisions of the *Privacy Act* to apply only to certain types of *ex parte* submissions, thereby permitting a court to conduct other parts of a hearing in public (*Ruby*, above, at paras 58-60).)

[49] I also considered the practical difficulty that would have been associated with reconvening an appropriate number of the Court’s designated judges any time prior to October or November of this year. In addition, I was sensitive to the fact that the Attorney General’s legal submissions had already been filed with the Court when I initially expressed an interest in the possibility of having an open hearing of all or part of the oral legal submissions in this proceeding. I was also mindful of the fact that it would have been unprecedented to have such an open hearing in respect of an application for warrants under section 21 of the Act. Assuming that section 27 does not preclude the holding of a public hearing in some circumstances, I considered that it would be preferable for such a hearing to be held in a proceeding that had been better planned for that purpose. Finally, at the time I was not entirely convinced that the factual and

[56] In contrast to the facts that are known by CSIS at the time it conducts a CSS operation for the purpose described above, when CSIS uses a CSS to geo-locate an individual, it knows one or more of that person's IMSI or IMEI identifiers, but not the individual's location. [REDACTED]

[REDACTED] specified that CSIS does not seek to geo-locate individuals through the use of CSS operations without a warrant.

[57] According to [REDACTED] TSPs are able to identify mobile devices that are allowed access to their services through two unique pieces of information that are provided by such devices, namely, the IMSI and the IMEI. [REDACTED] described those identifiers in his affidavit as follows:

13. An IMSI is a 15 digit string that uniquely associates to a TSP a subscriber account. It is comprised of three parts; a 3 digit Mobile Country Code (MCC) identifying the country of the IMSI subscriber; a 2 or 3 digit Mobile Network Code (MNC) identifying the home network of the IMSI subscriber; and the remaining digits ascribed to a Mobile Subscriber Identification Number (MSIN) which is associated by the service provider to uniquely identify a user's account within a provider's system.

14. An IMEI is a 15 digit string that uniquely identifies a cellular device, the actual hardware, to a TSP [...] The first 8 digits of an IMEI is comprised of a Type Allocation code (TAC) which identifies the make and model of the equipment. The following 7 digits are the serial number which uniquely identifies the device.

[58] By way of example, [REDACTED] gave the following IMSI number 302720123456789.

In this sequence, the digits "302" represent the MCC (country code of the subscriber); the digits "720" represent the MNC (network code of the subscriber's TSP); and the remaining digits represent the MSIN (unique subscriber identifying number). This information is stored on the SIM cards of mobile devices.

[59] By way of further example, [REDACTED] gave the following IMEI number:

353778081234560. In this sequence, the numbers “35377808” represent the TAC (device make and model), while the numbers “1234560” represent the unique device serial number. The Court understands that this information is stored on the device itself, rather than on its SIM card.

[60] [REDACTED]

[technical information]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[61] [REDACTED]

[technical information]

[REDACTED]

[62] To facilitate the provision of telecommunications services by TSPs, each TSP is licensed to operate and broadcast on frequencies that are different from those licensed to other TSPs.

[technical information] [REDACTED]

[63] [REDACTED]

[technical information] [REDACTED]

[64] By mimicking a TSP's cell tower, CSS devices induce cellular devices to interact with them as if they were a *bona fide* cell tower. In essence, a CSS is a "false" tower that requests devices to authenticate themselves to something that is posing as a TSP's tower.

[65] [REDACTED]

[technical information]

[REDACTED]

[66] To then identify the IMSI and IMEI identifiers that correspond to the device used by the subject of the CSS operation, [REDACTED]

[technical information]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[67] [REDACTED]

[technical information]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[68] [REDACTED]

[REDACTED] [technical information]

[69] [REDACTED]

[REDACTED] [technical information]

[70] [REDACTED]

[REDACTED] [technical information]

[71] [REDACTED]

[technical information]

[72] [REDACTED] CSIS operates its CSS equipment in a manner that does not degrade or otherwise affect in any perceptible way the quality of service experienced by the user of a mobile device that is in the vicinity of a CSS. [REDACTED]

[technical information]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[73] [REDACTED] further assured the Court that, with one exception, the CSS technology used by CSIS does not have any capacity to capture either the content of any communications made by users of mobile devices, or the information stored on their mobile devices. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]² [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[74] Finally, [REDACTED] stressed that the IMEI and IMSI identifiers that are captured by CSS equipment is not encrypted, but rather is “in the open.”

VI. CSIS’s Policy Regarding the Collection and Retention of Electronic Identifiers

[75] On [REDACTED] CSIS DDO issued a Directive relating to the collection and retention of electronic identifiers. According to [REDACTED] that Directive was issued as a result of Justice Noël’s decision in *X (Re)*, above, where he decided, among other things, that the words “strictly necessary” in section 12 of the Act apply to both the collection and the retention of information by CSIS.

[76] For the purposes of the Directive, electronic identifiers include IMSI and IMEI numbers,

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

² [REDACTED] testified that there is some CSS technology that is capable of intercepting the content of telephone calls, however, CSIS does not possess or use such technology. I expect that if CSIS ever acquires such technology, it will seek a warrant from the Court prior to using it, as the interception of such content clearly requires prior judicial authorization.

[77] Pursuant to the Directive, a moratorium was imposed on the use of technical means for the purpose of collecting electronic identifiers. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[78] According to [REDACTED] all of those electronic identifiers previously obtained by CSIS pursuant to CSS operations, including those for which an operational report has been written, have now been destroyed in accordance with the Directive. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[79] By way of further background, the Attorney General explained during the evidentiary hearing in this application that, given Justice Noël's decision in *X (Re)*, above, and given CSIS's view that the retention of IMSI and IMEI identifiers cannot be said to be "strictly necessary" once an operational report of the collection exercise has been finalized, those identifiers are generally deleted at that time. [REDACTED] testified that the operational reports are usually prepared "within [REDACTED] days." However, he added that, once CSS operations have been resumed following the issuance of these Judgment and Reasons, CSIS is considering requesting up to [REDACTED] months within which to determine whether IMSI and IMEI identifiers that it has collected can be attributed to a

subject of investigation. That is the period of time within which Justice Noël determined, in *X (Re)*, above, at para 253, that “information that is evidently not threat related and that does not involve the target” must be destroyed. [REDACTED]

[REDACTED]

[REDACTED]

VII. Assessment of Legal Submissions

[80] The Attorney General submits that CSIS’s use of CSS technology solely to capture IMSI and IMEI identifiers does not contravene either the *Radiocommunication Act*, the *Criminal Code*, or the *Charter*. I agree, subject to the reasons set forth below.

[81] The Attorney General’s submissions in respect of each of those laws will be addressed separately below.

A. *The Radiocommunication Act*

[82] The *Radiocommunication Act* governs the use of radio apparatus and radio-sensitive equipment to ensure the orderly development and efficient operation of radiocommunications in Canada. To this end, paragraph 5(1)(a) of that legislation allows the Minister of Industry (now the Minister of Innovation, Science and Economic Development) to issue licences and certificates to govern radio apparatus, including “any other authorization relating to radiocommunication that the Minister considers appropriate.”

[83] Among other things, paragraph 9(1)(b) of the *Radiocommunication Act* prohibits anyone from interfering with or obstructing any radiocommunication “without lawful excuse.”

[84] The Attorney General concedes that a CSS device is a “radio apparatus” within the meaning of the *Radiocommunication Act*. However, she maintains that CSIS’s use of a CSS complies with that legislation because CSIS holds an Authority to Use Radio [Authority], which was issued on September 1, 1992. She further maintains that, by virtue of that Authority and section 12 of the Act, CSIS’s use of CSS technology does not contravene paragraph 9(1)(b) of the *Radiocommunication Act*.

[85] For the present purposes, the provisions in the Authority which are most relevant are the following:

1) In accordance with subparagraph 5(1)(a)(v) of the *Radiocommunication Act*, this constitutes authorization for the Canadian Security Intelligence Service (CSIS) in respect of any and all types of specially designed radio apparatus used for the purpose specified in paragraph 2, for which a radio licence, under subparagraph 5(1)(a)(i) of the *Radiocommunication Act*, is not appropriate.

2) This authorization applies to radio apparatus specified in paragraph 1 only when it is being tested, used for training, or used for operations, solely in relation to investigations under sections 12 and 16 of the *Canadian Security Intelligence Services Act*, RSC 1985, c C-23.

[...]

7) All radio apparatus covered by this authorization shall not cause harmful interference to other authorized or licensed radio apparatus.

[...]

9) This authorization is valid unless withdrawn by the Department of Communications or the Canadian Security Intelligence Service (CSIS) indicates in writing that it is no longer required.

(Emphasis added.)

[86] The full text of the Authority is set forth in Appendix I to these Judgment and Reasons.

[87] The *Amici* note that CSIS was not “exposed to” CSS technology [REDACTED]. They maintain that it cannot reasonably have been in the Minister’s contemplation in 1992, at the dawn of cellular technology, that the Authority would be interpreted to authorize the use of CSS equipment for the purpose of obtaining IMSI and IMEI identifiers. They add that, had CSIS sought authorization from the present Minister, the Minister would likely have circumscribed its use of CSS technology, as he did in the authorization that was provided to the RCMP on March 13, 2017. The full text of that authorization is set forth in Appendix II to these Judgment and Reasons.

[88] The foregoing may all very well be true. However, it fails to come to grips with the fact that, on its face, the wording of the Authority is sufficiently broad to cover the use of CSS equipment by CSIS.

[89] Specifically, the use of such equipment would clearly fall within the scope of the words “in respect of any and all types of specially designed radio apparatus used for the purposes specified in paragraph 2,” as they appear in paragraph 1 of the Authority. I am inclined to agree

with CSIS that those words appear to have contemplated that the Authority would be used in respect of radio apparatus that was not yet in existence in 1992, when the Authority was issued.

[90] In any event, those words have the effect of allowing the Authority to be used in respect of such radio apparatus. Until the Minister withdraws the Authority, as provided for in paragraph 9, the Authority will remain sufficient authorization, for the purposes of the *Radiocommunications Act*, for CSIS to use CSS equipment. The evidence adduced in this proceeding is that the Minister has not taken any such action.

[91] I pause to observe that the Attorney General noted that, prior to obtaining the above-mentioned authorization in March of this year, the RCMP had been relying upon a different authorization pertaining to “jammers,” to conduct its CSS operations.

[92] The *Amici* added that the use of a CSS to obtain IMSI and IMEI identifiers associated with cellular devices clearly does cause some interference with those devices and has the potential to cause harmful interference, within the meaning of paragraph 7 of the Authority. In this regard, they note that “harmful interference” is defined in section 2 of the *Radiocommunication Act* to mean:

Radiocommunication Act,
RSC, 1985, c R-2

[...] an adverse effect of
electromagnetic energy from
any emission, radiation or

*Loi sur la
radiocommunication*,
LRC, ch R-2

[Brouillage préjudiciable] :
Effet non désiré d’une énergie
électromagnétique due aux

induction that	émissions, rayonnements ou inductions qui compromet le fonctionnement d'un système de radiocommunication relié à la sécurité ou qui dégrade ou entrave sérieusement ou interrompt de façon répétée le fonctionnement d'appareils radio ou de matériel radiosensible.
(a) endangers the use or functioning of a safety-related telecommunication system, or	
(b) significantly degrades or obstructs, or repeatedly interrupts, the use or functioning of radio apparatus or radio-sensitive equipment.	

[93] The *Amici* further note that the potential to cause harmful interference, including interfering with emergency calls to 911, formed part of the record before Justice Code of the Ontario Superior Court of Justice in *R v Brewster*, 2016 ONSC 4133, at paras 34, 38, 51–52. However, the passages from that decision that were cited by the *Amici* simply described (i) measures that the RCMP adopt, in operating its CSS equipment, to minimize the potential to cause unreasonable interference with mobile telephones, (ii) the capacity of *that* equipment to interrupt calls for up to two minutes (when configured in a rarely used mode), and (iii) arguments regarding alleged deficiencies in the RCMP's warrant, which Justice Code did not accept. Moreover, it bears underscoring that Justice Code's observations were made based on the specific evidence that was adduced in that case.

[94] The evidence in this case is that the equipment used by CSIS [REDACTED]

[REDACTED] [maintains contact with a mobile device for a few seconds]

[REDACTED]

[REDACTED] In my view, [REDACTED] do not

constitute significant degradations or obstructions, and do not constitute repeated interruptions, as contemplated by the above-quoted language from section 2 of the *Radiocommunications Act*.

[95] Given the foregoing, I am satisfied that CSIS's use of CSS technology does not contravene the *Radiocommunication Act*.

B. *The Criminal Code*

[96] Part VI of the *Criminal Code* provides a scheme that governs the interception of private communications. Among other things, section 184 of the *Criminal Code* prohibits the wilful interception of private communications by means of any electro-magnetic, acoustic, mechanical or other device, where done without consent or prior judicial authorization.

[97] CSIS maintains that its use of a CSS without prior judicial authorization does not contravene section 184 of the *Criminal Code* because its CSS equipment does not intercept any private communications. [REDACTED]

[REDACTED]

[REDACTED]

[98] Pursuant to section 183 of the *Criminal Code*, *private communication* is defined to mean:

Criminal Code, RSC 1985,
c C-46

Code criminel, LRC (1985),
ch C-46

[...] any oral communication,
or any telecommunication, that
is made by an originator who

[Communication privée]
Communication orale ou
télécommunication dont

is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it.	l'auteur se trouve au Canada, ou destinée par celui-ci à une personne qui s'y trouve, et qui est faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers. La présente définition vise également la communication radiotéléphonique traitée électroniquement ou autrement en vue d'empêcher sa réception en clair par une personne autre que celle à laquelle son auteur la destine.
---	--

[99] Pursuant to section 183 of the *Criminal Code*, the word *intercept* “includes to listen to, record or acquire a communication or acquire the substance, meaning or purport thereof.” It is common ground between CSIS and the *Amici* that obtaining IMSI and IMEI identifiers through the use of CSS equipment does not do any of these things, or otherwise capture any content of communications made by the mobile devices that are targeted by that equipment.

[100] Accordingly, the *Amici* agree that in the absence of any interception of the content of communications, CSIS’s use of CSS technology to attribute IMSI and IMEI identifiers to a subject of investigation does not contravene Part VI of the *Criminal Code*.

[101] However, the *Amici* maintained that CSIS’s use of a CSS without a warrant contravenes the mischief provisions in section 430 of the *Criminal Code*, and that neither section 12 of the

Act nor the Authority discussed at paragraphs 84-90 above provide a lawful exemption from section 430. I disagree.

[102] Subsection 430(1) states:

Criminal Code, RSC 1985,
c C-46

430 (1) Every one commits
mischief who wilfully

(a) destroys or damages
property;

(b) renders property
dangerous, useless, inoperative
or ineffective;

(c) obstructs, interrupts or
interferes with the lawful use,
enjoyment or operation of
property; or

(d) obstructs, interrupts or
interferes with any person in
the lawful use, enjoyment or
operation of property.

Code criminel, LRC (1985),
ch C-46

430 (1) Commet un méfait
quiconque volontairement,
selon le cas :

a) détruit ou détériore un bien;

b) rend un bien dangereux,
inutile, inopérant ou inefficace;

c) empêche, interrompt ou
gêne l'emploi, la jouissance ou
l'exploitation légitime d'un
bien;

d) empêche, interrompt ou
gêne une personne dans
l'emploi, la jouissance ou
l'exploitation légitime d'un
bien.

[103] Pursuant to section 429 of the *Criminal Code*, “no person shall be convicted of an offence under sections 430 to 446 where he proves that he acted with legal justification or excuse and with colour of right.”

[104] For the reasons set forth in Part VII.A. immediately above, I do not accept the *Amici*'s position that the Authority does not provide such legal justification.

[105] For the reasons that are provided in Part VII.C.(2)(b)(ii) below, I do not accept the *Amici*'s position with respect to section 12.

[106] I will simply add in passing that, in their oral submissions, the *Amici* conceded that if I find that section 12 provides sufficient authorization for the capture of IMSI and IMEI identifiers through the use of CSS technology, that would be sufficient to bring that activity within the scope of the defence afforded by section 429 of the *Criminal Code*.

C. *Section 8 of the Charter*

(1) Legal principles

[107] Section 8 of the *Charter* provides: "Everyone has the right to be secure against unreasonable search or seizure."

[108] It follows that there are two distinct issues to be assessed in determining whether there has been a violation of section 8, namely (i) whether there has been a "search or seizure," and (ii), if so, whether that search or seizure was "unreasonable," (*R v Gomboc*, 2010 SCC 55, at para 20 [*Gomboc*]).

[109] In approaching these issues, courts must adopt "a purposive approach that emphasizes the protection of privacy as a prerequisite to individual security, self-fulfilment and autonomy as

well as to the maintenance of a thriving democratic society” (*R v Spencer*, 2014 SCC 43, at para 15 [*Spencer*]).

(a) *What Constitutes a Search or Seizure?*

[110] A “seizure” has been defined as “the taking of a thing from a person by a public official without that person’s consent” as well as the compelled production of information, for example, pursuant to a regulatory statute (*Thomson Newspapers Ltd v Canada (Director of Investigation and Research, Restrictive Trade Practices Commission)*, [1990] 1 SCR 425, at 505 [*Thomson Newspapers*]; *R v McKinlay Transport Ltd*, [1990] 1 SCR 627, at 642 [*McKinlay*]).

[111] By contrast, a “search” occurs when an individual who is the object of intrusive state activity has a reasonable expectation of privacy in the subject matter of the alleged search. If so, then the activity in question constitutes a “search” and section 8 is engaged (*Spencer*, above, at para 16; *Gomboc*, above, at para 20).

[112] In assessing whether an individual had a reasonable expectation of privacy in relation to the subject matter of an alleged search, the totality of the circumstances to be assessed include various factors directly related to the individual’s expectation of privacy, both subjectively and objectively viewed. These include:

- i. the subject matter of the alleged search;
- ii. the individual’s interest in the subject matter;

- iii. the individual's subjective expectation of privacy in the subject matter; and
- iv. whether the individual's subjective expectation of privacy was objectively reasonable, having regard to the totality of the circumstances.

(*Spencer*, above, at para 18).

[113] With respect to the first of the four factors listed above, an assessment must be made of both the subject matter of the alleged search or seizure, as well as any inferences that can reasonably be made from that subject matter regarding private activities or other private information of the individual (*Spencer*, above, at paras 26–31). Put differently, when the subject matter of an alleged search is information, a Court must consider the significance of the information obtained as a result of the search (*R v AM*, 2008 SCC 19, at para 38 [*AM*]).

[114] The protection afforded by section 8 of the *Charter* does not extend to all matters that the individual may wish to keep out of the hands of agents of the state (*R v Tessling*, 2004 SCC 67, at para 26 [*Tessling*]). Rather, that protection is limited to a “biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state [including] information which tends to reveal intimate details of the lifestyle and personal choices of the individual” (*R v Plant*, [1993] 3 SCR 281, at 293 [*Plant*] (emphasis added); *Spencer*, above, at para 27).

[115] In evaluating the second of the above-listed factors (the individual's interest in the subject matter of the alleged search), the focus is upon the extent to which that interest may be said to be

direct (*Tessling*, above, at para 32; *Spencer*, above, at para 19; *R v Patrick*, 2009 SCC 17, at para 27 [*Patrick*]).

[116] With respect to the third of those factors (the individual's subjective expectation of privacy in the subject matter), this may be established by direct evidence demonstrating such an expectation, or by inference from the circumstances (*Spencer*, above, at para 19; *Tessling*, above, at para 38). For example, a subjective expectation of privacy can be presumed in respect of activities that take place in a person's home (*Patrick*, above, at para 37; *Gomboc*, above, at para 25). However, section 8 of the *Charter* "does not cloak the home in an impenetrable veil of privacy," and where there is no direct search of the home itself, "the informational privacy interest should be the focal point of the analysis" (*Gomboc*, above, at paras 46, 49). In this latter regard, the fact that the home may have been involved "should be subsidiary to what the investigative technique was capable of revealing about the home and what information was actually disclosed" (*Gomboc*, above, at para 50).

[117] Turning to the fourth of the factors (whether the individual's subjective expectation of privacy was objectively reasonable), the degree of privacy a citizen can reasonably expect may vary significantly depending upon the activity that brings him or her into contact with the state (*Thomson Newspapers*, above, at 506-507).

[118] The considerations to be assessed in evaluating this factor include:

- i. the nature of the privacy interest at stake;

- ii. the circumstances in which the search occurred;
- iii. the place in which it occurred;
- iv. whether the information has already been abandoned or disclosed to third parties;
- v. the purpose of the intrusion;
- vi. the extent to which the search technique that was used was intrusive in relation to the identified privacy interest;
- vii. the relevant statutory and contractual framework, if any; and
- viii. whether the use of the search or surveillance technology that was used was itself objectively unreasonable.

(*Spencer*, above, at para 20; *Tessling*, above, at para 32; *Patrick*, above, at para 38)

[119] The Supreme Court has also held the view in the past that the nature of the state's interest in conducting a particular type of intrusive activity can also be considered in determining whether that activity constitutes a "search" (*R v Evans*, [1996] 1 SCR 8, at para 40 [*Evans*]; *R v Colarusso*, [1994] 1 SCR 20, at 53 [*Colarusso*]). However, it has since stated that it is more logical to consider this factor when considering whether a search was unreasonable (*Tessling*, above, at para 64, discussing the seriousness of the offence).

[120] Insofar as the nature of the privacy interest at stake is concerned, privacy interests can be primarily territorial, personal or informational in nature. These are not strict or mutually

exclusive categories (*Spencer*, above, at para 35; *Tessling*, above, at para 20). The analysis of these categories “turns on the privacy of the area or thing being searched and the impact of the search on its target, not on the legal or illegal nature of the items sought” (*Spencer*, above, at para 36).

[121] Territorial privacy includes an individual’s privacy in an area or place, such as his or her home, hotel room or place of work. Personal privacy connotes a person’s bodily integrity, and in particular the right not to have his or her body touched, explored or sampled to disclose objects or information an individual may wish to conceal. Informational privacy includes privacy in information that an individual may want to keep secret or to be kept in confidence, information over which an individual may wish to maintain control, and information that has been provided to others on an anonymous basis or that is related to activities in which the individual has engaged on an anonymous basis (*Spencer*, above, at paras 38-44).

[122] The factors to be considered in determining the parameters of the protection afforded by section 8 with respect to informational privacy include the nature of the information in question, the place where the information was obtained, the manner in which it was obtained and the seriousness of the state interest in question (*Plant*, above, at 293). Additional factors that must be considered include:

- i. whether the subject matter of the search was in public view;
- ii. whether the subject matter had been abandoned;

- iii. whether the use of surveillance technology was itself objectively unreasonable; and
- iv. whether any intimate details of the individual's lifestyle, or core biographical information of the individual, were obtained.

(*Tessling*, above, at para 32).

[123] With respect to the relevant statutory framework referred to at paragraph 118 above, the objective reasonableness of a person's privacy expectation will vary according to the nature of that framework, for example, whether it is criminal, administrative, regulatory or national security legislation. In brief, the objective privacy expectations will be much greater in a criminal context than they often will be in an administrative or regulatory context (*Thomson Newspapers*, above, at 505–508; *Colarusso*, above, at 37-38, 40; *R v Jarvis*, 2002 SCC 73, at para 62 [*Jarvis*]). Stated differently, intrusion by the state that may constitute a search or a seizure in a criminal context may not constitute either of these things in a non-criminal context (*McKinlay*, above, at 641-642, 647-648; *R v Wholesale Travel Group Inc*, [1991] 3 SCR 154, at 226-227).

[124] Finally, where there is a relevant contractual framework, it will be appropriate to consider the nature of the relationship between the parties to the framework, whether the person in receipt of the information in question was contractually bound to keep the information confidential, and whether the relationship between that person and the individual whose privacy interests are at issue is one of confidence (*Plant*, above, at 294-295).

(b) *What Constitutes an Unreasonable Search or Seizure?*

[125] Section 8 of the *Charter* does not afford protection against all searches, only against *unreasonable* ones.

[126] Broadly speaking, a determination of whether a search is unreasonable requires assessing “whether in a particular situation the public’s interest in being left alone by government must give way to the government’s interest in intruding on the individual’s privacy in order to advance its goals” (*Hunter et al v Southam Inc*, [1984] 2 SCR 145, at 159–160 [*Hunter*]). In conducting such assessments, a court is often called upon to weigh the privacy interests of one or more individuals against the interests of public safety, including the right to life, liberty and security of persons who may be in danger of serious harm (*R v Tse*, 2012 SCC 16, at para 21 [*Tse*]).

[127] In brief, “[w] here the constitutional line of ‘reasonableness’ will be drawn [is] a function of both the importance of the state objective and the degree of impact on the individual’s privacy interest” (*R v Rodgers*, 2006 SCC 15, at para 27 [*Rodgers*]; *AM*, above, at paras 36–37).

[128] It follows that, “if a person has but a minimal expectation with respect to informational privacy, this may tip the balance in the favour of the state interest” (*Jarvis*, above, at para 71).

[129] In any event, the state’s intrusion on an individual’s privacy rights will only be upheld where it does not extend beyond what is necessary to achieve the state’s legitimate objective (*Thomson Newspapers*, above, at 495).

[130] Given that the underlying purpose of section 8 is to protect individuals from unjustified state intrusions upon their privacy, prior authorization of any such intrusions is presumptively required *before* they occur. Put differently, a search will be presumed to be unreasonable if it has not been pre-authorized by an entirely neutral and impartial arbiter who is capable of acting judicially in balancing the interests of the state against those of the individual (*Spencer*, above, at para 68; *Goodwin v BC (Superintendent of Motor Vehicles)*, 2015 SCC 46, at para 56 [*Goodwin*]; *Hunter*, above, at 160-162).

[131] In addition, the neutral arbiter must be satisfied that the person seeking the authorization has reasonable grounds, established under oath, to believe that the relevant statutory or other conditions to be met before the search power may be exercised have indeed been met (*Hunter*, above, at 166-168). In some contexts, including the national security context, this “reasonable grounds to believe” standard may be flexible (*Hunter*, above, at 168; *Rodgers*, above, at para 35; *R v Chehil*, 2013 SCC 49, at para 23 [*Chehil*]). For example, a high degree of accuracy may justify the imposition of a lower evidentiary standard – such as reasonable suspicion – to trigger the availability of the search power (*Goodwin*, above, at para 67). This is particularly so where the intrusion is minimal and narrowly targeted (*AM*, above, at paras 13, 42; *R v Kang-Brown*, 2008 SCC 18, at paras 25, 60, 210, 213 [*Kang-Brown*]; and *Chehil*, above, at para 28). In such circumstances, the person who conducted the search after having satisfied the reasonable suspicion test may not require pre-authorization by a neutral arbiter at all (*Kang-Brown*, above; *Mahjoub (Re)*, 2013 FC 1096, at para 35 [*Mahjoub*]).

[132] Where pre-authorization is presumptively required, it will fall to the person who conducted a warrantless search to justify why it was not feasible to obtain such pre-authorization (*Kang-Brown*, above, at para 59).

[133] Alternatively, that person may overcome the presumption of unlawfulness that applies to warrantless searches by demonstrating that the search was authorized by law, that the law in question is reasonable, and that the manner in which the search was carried out was reasonable (*Goodwin*, above, at para 48; *Wakeling v United States of America*, 2014 SCC 72, at para 41 [*Wakeling*]; *Rodgers*, above, at para 25; *R v Collins*, [1987] 1 SCR 265, at 278).

[134] In assessing whether a law which authorizes a warrantless search is reasonable, factors to be assessed include its nature and purpose, the degree of intrusiveness that it authorizes, the mechanism of intrusion authorized, the extent to which it provides for judicial supervision, and any other accountability measures or “checks and balances” that it contains to constrain the extent of the state’s intrusion on an individual’s privacy interests (*Goodwin*, above, at paras 57 and 71-72; *Thomson Newspapers*, above, at 596–597; *Wakeling*, above, at para 77). Depending upon the circumstances and the legislative scheme, the availability of after-the-fact oversight may assist to overcome the presumptive unlawfulness of a warrantless search (*Goodwin*, above, at para 71).

[135] With respect to the manner in which a search is carried out, factors to be assessed include the reliability or accuracy of the search mechanism, and the extent to which it may intrude on the privacy of innocent individuals. In this latter regard, “[a] method of searching that captures an

inordinate number of innocent individuals cannot be reasonable” (*Goodwin*, above, at para 67 quoting *Chehil*, above, at para 51).

[136] In any event, a court must assess what the search mechanism or technology is currently capable of doing, as opposed to what it may be capable of doing in the future (*AM*, above, at paras 39–40; *Gomboc*, above, at para 40; *Tessling*, above, at para 29).

(2) Application of the Legal Principles to the Facts of this Application

(a) *Did CSIS’s Use of CSS Technology Constitute a “Search”?*

[137] In this case, CSIS used its CSS technology solely to intercept the IMSI and IMEI numbers from [REDACTED] mobile devices, so that it could then identify those specific devices and attribute them to him. CSIS did not use CSS technology to geo-locate [REDACTED]. Indeed, the Attorney General concedes that a warrant would be required to use CSS technology in that manner. Accordingly, the following assessment will be confined to assessing the use of CSS technology to capture the IMSI and IMEI numbers pertaining to [REDACTED] wireless devices, and thereby enable CSIS to identify those devices and attribute them to him.

[138] According to [REDACTED] the individual or individuals who are the subject of a CSS operation ordinarily are known [REDACTED]

[REDACTED] Therefore, it is important to keep in mind that CSIS will ordinarily already know certain things about such individuals at the time the CSS operation is conducted. Those things include their location [REDACTED]

[REDACTED] even though their [REDACTED]
[REDACTED] may not yet be known.

[139] In passing, I will pause to recall that, with one exception, the CSS equipment currently operated by CSIS is not capable of intercepting the content of any communications. [REDACTED]

[REDACTED]

[REDACTED] The evidence on the record is that CSIS has a policy of not capturing such content. In my view, any such activity would require a warrant.

[140] The Attorney General submits that CSIS's use of CSS technology to obtain the IMSI and IMEI identifiers pertaining to an individual's mobile device does not engage section 8 of the *Charter* because individuals generally do not have a reasonable expectation of privacy in respect of those identifiers. I disagree. In my view, a consideration of the totality of the circumstances, which are addressed below, and taking a purposive approach to section 8 of the *Charter*, suggests that individuals do have a reasonable expectation of privacy in respect of those numbers. This is because of the nature of the information that those numbers permit CSIS to obtain or infer. Therefore, the use of CSS technology constitutes a "search" and the first of the two elements in section 8 is met.

(i) The Subject Matter of the Intrusive Activity

[141] The Attorney General maintains that the IMSI and IMEI identifiers obtained through the use of CSS technology are "just mundane numbers" that simply reveal the country code of the

subscriber, the identity of the subscriber's TSP, the subscriber's unique identifying number, the mobile device's make and model, and the device's serial number. The Attorney General adds that this information reveals nothing about an individual's biographical core or private life, and does not tend to reveal any intimate details of the lifestyle and personal choices of the individual. For example, in this application, the CSS operation revealed [REDACTED]

[REDACTED]

[REDACTED]

[142] In support of its position that this information does not engage section 8 of the *Charter*, the Attorney General places significant reliance on *Tessling*, *Gomboc* and *Plant*, above, where the Supreme Court of Canada concluded that the capture of information pertaining to the amount of heat emanating from a home, the amount of electricity flowing into a home, and records pertaining to the amount of electricity consumed in a home, respectively, did not engage section 8.

[143] However, a senior employee of CSIS, [REDACTED] [REDACTED] stated in an affidavit that "[o]ver time, the IMSI and IMEI numbers of a specific subject of investigation may reveal patterns" (emphasis added). [REDACTED]

[REDACTED]

[144] Although [REDACTED] did not mention it, another example of information that could well be revealed through the capture of a subject of investigation's IMSI or IMEI numbers could be that

individual's pattern [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] This may well have been what [REDACTED] was referring to

when he testified that IMSI and IMEI information is required “in order to be able to determine

[REDACTED] [contacts] and communication patterns and a bunch of other additional elements in regards

to undergoing national security investigations.” [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] the capture of IMSI and IMEI identifiers can be distinguished from what was at issue in

Tessling, Gomboc and Plant, above.

[145] In addition, in a report that was entered as Exhibit 16 in this proceeding, it was noted that

“IMSI/IMEI identifiers can also be used to identify digital activities such as web browsing [...]

without any need to ever match a compiled profile to an individual's specific name or address.”

(Tamir Israel & Christopher Parsons, *Gone Opaque? An Analysis of Hypothetical IMSI Catcher*

Overuse in Canada, (Ottawa: Telecom Transparency Project & Samuelson-Glushko Canadian

Internet Policy & Public Interest Clinic, 2016, at 15 [*Gone Opaque*]).

[146] It is also significant that ██████ further noted that, “[l]ike any other type of intelligence the Service collects, an IMSI or IMEI obtained through a CSS device may be shared with foreign agencies where the Service considers it to be appropriate.” He added: “Prior to sharing this information, the Service will assess and examine options to mitigate any potential risks of mistreatment of those persons whose identities are disclosed to the foreign agencies.” In this regard, he stated that he was aware of ██████ instances where the IMSI and/or IMEI numbers collected by CSIS through the use of CSS technology were shared with foreign agencies. I will address the potential significance of such sharing of information with foreign authorities at paragraph 168 below.

(ii) Individuals’ Interest in the Subject Matter

[147] ██████ clearly has a direct interest in the IMSI and IMEI identifiers associated with the mobile devices that were captured by CSIS’s CSS operation. The same would be true for other subjects of a CSIS investigation, who may be targets of a CSS operation, regardless of whether their identities may be known. The Attorney General did not suggest otherwise.

(iii) Do Individuals Have a Subjective Expectation of Privacy in the Subject Matter?

[148] No evidence was tendered in this proceeding with respect to the subjective expectations of ██████ or others in respect of the IMSI and IMEI identifiers associated with their mobile devices. However, this question does not pose a “high hurdle” (*Patrick*, above, at para 37).

I agree with the *Amici* that it can be assumed that individuals in general likely have a subjective expectation that any information concerning their mobile devices that may be communicated to

the cell towers operated by their TSPs will not be surreptitiously captured by agents of the state, such as CSIS, or indeed by others through the use of “false” cell towers. That said, most individuals likely are not aware that any information that has the potential to reveal personal information about them is “offered” by their mobile devices to cell-towers, and may be intercepted by agents of the state.

(iv) If So, Are Such Expectations Objectively Reasonable?

The Nature of the Privacy Interest at Stake

[149] The principal privacy interests implicated by CSIS’s use of CSS technology to capture IMSI and IMEI identifiers are the interests of individuals in their personal information pertaining to their mobile electronic devices and their use of those devices. Those interests are engaged upon CSIS’s initial “grab” of their IMSI and IMEI numbers, and then when CSIS subsequently uses those numbers to build a profile of the individual’s [contacts] and communication patterns.”

[150] To the extent that such technology can reveal information about whom subjects of investigation are communicating with when they are at different locations, [redacted] [redacted] the use of that technology also implicates an element of territorial privacy. In the particular circumstances of this case, territorial privacy is very much secondary to informational privacy (*Spencer*, above, at para 37; *Gomboc*, above, at para 49). This is because CSIS generally knows the location of its subject of investigation at the time it conducts a CSS operation to capture the IMSI and IMEI identifiers associated with the wireless device(s) carried by that individual.

[151] Within the broad umbrella of informational privacy, the interests that are implicated by CSIS's capture and subsequent analysis of IMSI and IMEI numbers are the confidentiality of those numbers, the subject of investigation's control over who has access to those numbers, and that individual's interest in preserving the anonymity of (i) his links with the people with whom he or she may be communicating, and (ii) the location(s) at which such communications may be taking place [REDACTED] (*Spencer*, above, at paras 42–49).

The Circumstances in which IMSI and IMEI Identifiers Are Obtained

[152] According to [REDACTED] CSIS deploys CSS technology to obtain IMSI and IMEI identifiers for the purposes of attributing a mobile device to a specific subject of an investigation being conducted pursuant to section 12 [REDACTED]. As previously mentioned, at the time CSS operations are conducted, such individuals typically are targets of CSIS, such that various things are already known about them, including their location, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] the personal identities of subjects of investigation are typically already known at the time CSIS conducts its CSS operations.

The Manner and Place of the Capture of IMSI and IMEI Identifiers

[153] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[154] [REDACTED]

[REDACTED]

[REDACTED]

[155] Regardless of where the subject of investigation may be located, CSIS's capture of the IMSI/IMEI numbers of that individual's mobile device(s) through the use of CSS technology does not reveal anything more about that individual's mobile device or activities within that venue [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[156] As explained at paragraphs 70-73 and 79 above, the evidence in this proceeding is that the CSS equipment used by CSIS maintains contact with an individual's mobile device [REDACTED]

[for a few seconds] [REDACTED]

[REDACTED]

[REDACTED] In addition, CSIS operates its CSS equipment in a manner that does not degrade or

otherwise affect in any perceptible way the quality of service experienced by the user of a device that is in the vicinity of a CSS. In addition, with one exception, the CSS equipment does not have the capacity to capture either the content of any communications made by the users of mobile devices, or the information stored on their mobile devices. The one exception relates to the

[REDACTED]

[REDACTED]

[REDACTED] Finally, CSIS deletes the information that was captured from the mobile devices of third parties during its CSS operations very quickly, often within [REDACTED] days, and in any event as soon as an operational report has been written with respect to a given CSS operation.

[157] The manner in which CSS operations are conducted is such that the subject of investigation generally would not be aware that he or she is the target of such an operation, although he or she may suspect that this is the case.

Whether the IMSI/IMEI Identifiers have been Abandoned or Disclosed to One or More Third Parties

[158] The Attorney General places significant emphasis upon the fact that the IMSI and IMEI numbers that are obtained through CSS operations are captured from the public airwaves, in a context in which that information is being “offered” to cell towers by the mobile device(s) of the subject of investigation. In this regard, the Attorney General draws a parallel between the IMSI and IMEI identifiers that are “voluntarily” provided to TSPs, and the electricity consumption information that was provided to electricity providers in *Plant*, above. The Attorney General also

draws a parallel to cases such as *Patrick*, above, where it was found that a reasonable expectation of privacy did not exist in respect of information that had been “abandoned” in the garbage.

[159] However, in my view, the average person likely would consider his or her IMSI and IMEI identifiers to be more personal and confidential than electricity consumption data,

[REDACTED]

[REDACTED]

[160] In addition, as with the heat emanating from their home, the average person likely would not consider his or her IMSI and IMEI identifiers to have been “abandoned” when they are disclosed to cell towers by their mobile device(s) (*Tessling*, above, at para 41). In contrast to garbage, which they are aware will eventually find its way to a municipal dump that may be accessible by persons who are not associated with the garbage collection and disposal process, the average person is likely to consider that his or her IMSI and IMEI identifiers will remain confidential as between them and their TSP, unless police obtain a warrant to obtain such information from their TSP. Moreover, in contrast to the implied waiver of privacy rights that may be said to be given to allow members of the general public to approach one’s home for a purpose that would be considered by the homeowner to be legitimate (*Evans*, above, at paras 6, 14), there is no similar implied waiver of a person’s privacy rights in his or her IMSI and IMEI identifiers vis-à-vis the general public, when their mobile device offers that information to the cellular environment.

The Extent to which the Search Technique is Intrusive in Relation to the Identified Privacy Interest

[161] In my view, CSS technology is minimally intrusive in respect of individuals' informational and territorial privacy interests. Initially, all that is obtained are "bare" IMSI and IMEI numbers that simply reveal the identity of an individual's TSP, the individual's Mobile Subscriber Identification Number, the make and model of the mobile device in question, and its serial number. Neither the mobile device nor its contents are accessed in any way. Likewise, no information that that might be available through the device is captured, and, with the one exception [REDACTED] CSIS cannot access the content of communications made on the mobile device.

[162] [REDACTED]
[REDACTED]
begin to put together an initial profile of the subject of investigation's [contacts] and communication patterns." It is this very information that may assist CSIS to establish the "reasonable grounds to believe" required to obtain a warrant, as set forth in subsections 21(1), 21(3), 21(3.1), 21.1(1), 21.1(3) and 21.1(4) of the Act, or the renewal of a warrant under section 22. [REDACTED]

[REDACTED]
[REDACTED]

[163] Although CSIS may be able to begin putting together an initial profile of the subject of investigation's [contacts] and communications patterns, it is difficult to see how the

inferences that it may be able to draw regarding the individual's personal activities would be particularly strong or invasive. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The Relevant Statutory and Contractual Framework

[164] The relevant statutory framework within which CSIS conducts CSS operations for the purposes of attributing a wireless device to a known subject of investigation is the mandate that it has been accorded by section 12 of the Act. Pursuant to that provision, CSIS is required to collect, to the extent that is strictly necessary, and analyze and retain information and intelligence in respect of activities that may, on reasonable grounds, be suspected of constituting threats to the security of Canada. For the reasons explained at paragraph 119 above, I will consider the state's interest in its security at the second stage of the analysis contemplated by section 8 of the *Charter*, which is addressed in Part VII.C.(2)(b) below. For now, I will continue to focus solely on the perspective of individuals who may be subject to intrusive activities by CSIS under section 12 of the Act.

[165] The Attorney General maintains that the national security context in which CSS operations may be deployed is closer to the regulatory and administrative contexts than to the criminal law context. In essence, the Attorney General appears to maintain that individuals have a lower expectation of privacy in the national security context than in the criminal context,

because the former context often does not result in criminal prosecutions against individuals, thereby engaging individuals' liberty interests. In other words, there is a lower possibility of individuals ultimately being prosecuted in whole or in part on the basis of personal information that CSIS may capture than there is of them being prosecuted on the basis of similar information that the police might capture.

[166] In my view, this alone does not provide a sufficient basis for concluding that individuals have a lower expectation of privacy in the national security context than in the criminal context.

[167] In assessing whether individuals have a reasonable expectation of privacy in respect of any personal information gathered by agents of the state, the relevance of the statutory context in which the information is gathered depends upon the severity of the potential consequences for those individuals (*Charkaoui v Canada (Citizenship and Immigration)*, 2008 SCC 38, at para 53 [*Charkaoui III*]), the nature of the conduct addressed by the legislation in question, and the purposes for which the legislation was enacted to regulate that conduct (*Thomson Newspapers*, above, at 495–496, 509–510).

[168] Insofar as potential consequences are concerned, CSIS's investigative activities under section 12 may very well lead to outcomes that are even more severe for individuals than in the criminal context (*Charkaoui II*, at para 54). This includes deportation to countries where they may face death or longer prison terms than they would potentially face in Canada. In addition, information captured by CSIS may not only be shared with law enforcement and other agents of the state in Canada, and ultimately lead to criminal charges, but also with foreign governments.

Indeed, as noted at paragraph 146 above, the possibility of this occurring with respect to IMSI and IMEI identifiers was specifically identified by ██████████. Among other things, this may have significant adverse consequences for individuals' ability to travel outside Canada and for their ability to obtain new employment or maintain their existing employment. Moreover, the stigma associated with being a subject of investigation under the Act is likely closer to that which is associated with being charged and convicted of serious crimes than it is to any stigma that might be associated with being charged and convicted of public welfare, regulatory or economic offences, even where a significant prison sentence is imposed (*Thomson Newspapers*, above, at 509–517).

[169] Turning to the nature of the conduct addressed by section 12 of the Act, I consider that most of the types of activities that are included within the definition of “threats to the security of Canada” that is set forth in section 2 of the Act are much closer to the “true” crimes that are the subject of criminal legislation, than to the typical offences that are established by public welfare, regulatory and economic legislation.

[170] Whereas the nature of the conduct addressed by the latter types of legislation is such that individuals can be taken to have accepted certain terms and conditions of entry into the economic/regulatory field, or upon their entry into the country, I do not think that the same can be said, at least not to the same degree, with respect to activities that may attract CSIS's intrusive scrutiny under section 12. While members of the public likely recognize and expect that CSIS will investigate threats to the security of Canada using some intrusive means, they also likely expect that it will do so only subject to safeguards that either protect their rights under the *Charter*, or that

place reasonable limits on intrusions on those rights. That is something that will be assessed in Part VII.C.(2)(b) of these reasons below.

[171] Regarding the purpose of the legislation, again, I consider the investigation of threats to the security of Canada pursuant to section 12 and the collection of information or intelligence pursuant to section 16 of the Act to be closer in nature to the purposes of criminal legislation than to the purposes underlying the types of public welfare, regulatory or economic legislation in respect of which low expectations of privacy have been found to exist (see e.g., *Thomson Newspapers*, above, at 505–506, 508–509, 515–516; *Comité paritaire de l'industrie de la chemise v Potash*; *Comité paritaire de l'industrie de la chemise v Sélection Milton*, [1994] 2 SCR 406, at 443-447; *Colarusso*, above, at 37-38, 40). Nevertheless, I accept that members of the public likely are prepared to accept *some* reduction in their privacy rights to enable CSIS to investigate activities that may, on reasonable grounds, be suspected of constituting threats to the security of Canada. However, in the absence of any submissions from the Attorney General or the *Amici* regarding the nature of such reductions of privacy, it is difficult for me to discuss in the abstract what they may be. In my view, these will likely need to be addressed over time, and assessed by reference to the totality of their respective contexts.

[172] Insofar as IMSI and IMEI identifiers are concerned, I am satisfied that those whose activities may be subject to investigation under section 12 of the Act, and whose anonymity interests may be implicated by what CSIS is able to do with that information, are not likely to have a reduced expectation of privacy. This is because of what they would likely believe, if they were fully informed, CSIS may be able to begin learning about their private activities upon

capturing that information. As I have mentioned, this can include beginning to build a personal profile on them that may extend to (i) determining “[contacts]” or communications patterns”

[REDACTED]

[REDACTED] (ii) drawing inferences about [them]

[REDACTED] CSIS has tremendous resources available to do these things, including its Operational Data Analysis Centre [ODAC], which was discussed in some detail in *X (Re)*, above, at paras 37 and following. In one passage, Justice Noël observed as follows:

The ODAC processes and analyzes data such as (but not limited to): [REDACTED]

[REDACTED] The end product is intelligence which reveals specific, intimate details on the life and environment of the persons the CSIS investigates. The program is capable of drawing links between various sources and enormous amounts of data that no human being would be capable of. [REDACTED]

[REDACTED]

(*X (Re)*, above, at para 42).

[173] I agree with the *Amici* that these potential encroachments on individuals’ anonymity distinguish the reasonable expectations of those whose activities may be subject to investigation or information gathering by CSIS, from the reasonable expectations of third parties whose IMSI and IMEI numbers are incidentally obtained in the course of a CSS operation and then destroyed before anything further is done with those numbers. As noted by the *Amici*, such early destruction of the IMSI and IMEI information of third parties serves to preserve the anonymity of those individuals, including the anonymity that is inherent in people’s use of their mobile devices.

[174] I will observe in passing that the Attorney General did not identify any legislation whatsoever, whether regulatory, economic or otherwise, that permits the surreptitious capture of otherwise inaccessible information about individuals' telephones without a warrant.

[175] Turning to the relevant contractual framework, no evidence was provided regarding the contractual obligations of TSPs towards their subscribers. However, I agree with the *Amici* that if the average person were aware that mobile devices disclose IMSI and IMEI identifiers to the cellular environment when they are in idle mode, he or she likely would believe that such information is only being disclosed to their TSP. This is in part due to the fact that individuals generally consider their phones to be private. This important consideration distinguishes the facts in this case from those in *Plant*, *Tessling* and *Gomboc*, above.

[176] Specifically, one of the factors that was considered to be particularly relevant by the Supreme Court in *Plant* was that members of the public at large could make inquiries to the municipal electricity commission in question concerning the electricity consumption at a particular address (*Plant*, above, at 294). In *Tessling*, a factor that appears to have been accorded significance was that the heat information that was captured by the police was obtained from the exposed external walls of the accused person's home, and some extent of heat emanating from a home "is obvious to even the most casual observer" (*Tessling*, above, at paras 41, 46–47). By contrast, the IMSI and IMEI identifiers associated with mobile devices are stored inside those devices, and only released to the cellular environment for the limited purpose of accessing the cellular network of an individual's TSP. Finally, in *Gomboc*, the Court placed considerable significance on the fact that paragraph 10(3)(f) of the *Code of Conduct Regulation* enacted

pursuant to the *Electric Utilities Act*, SA 2003, c E-5.1, permitted the disclosure of customer information “to a peace officer for the purpose of investigating an offence if the disclosure is not contrary to the express request of the customer.” Accordingly, the Court considered that Mr. Gomboc had been given “express notice that such cooperation might occur,” yet failed to request that his customer information be kept confidential (*Gomboc*, above, at paras 31, 33, 82 and 95).

[177] The *Amici* also referred to publicly available information, which I agree can be relevant to an assessment of the objective reasonableness of the subjective expectation that individuals likely have that the IMSI and IMEI numbers of their mobile devices will not be intercepted by agents of the state. In my view, the information in question lends support to the view that individuals have an objectively reasonable expectation of privacy in the IMSI and IMEI identifiers associated with their mobile devices.

[178] In particular, the *Amici* noted that the *Gone Opaque* publication discussed at paragraph 145 above reports that the protection of the confidentiality of IMSI identifiers was embraced by the European Telecommunications Standards Institute as one of its five security goals in respect of telephones operating on the Global System for Mobile Communications [GSM] system (*Gone Opaque*, above, at 9). The same page of that report also discusses the assignment of Temporary Mobile Subscriber Identity [TMSI] numbers to further protect the confidentiality of IMSI numbers, although it is not clear whether the use of such numbers is confined to Europe or extends to Canada.

[179] The *Amici* further referred to a page on Wikipedia entitled “International mobile subscriber identity,” which states: “To prevent eavesdroppers identifying and tracking the subscriber on the radio interface, the IMSI is sent as rarely as possible and a randomly generated TMSI is sent instead” (Wikipedia, “International mobile subscriber identity”, online: (2017) <https://en.wikipedia.org/wiki/International_mobile_subscriber_identity>).

[180] Although there is no evidence regarding [REDACTED] [REDACTED] the *Amici* submitted that the evidence of [REDACTED] regarding the circumstances in which IMSI and IMEI identifiers are released by mobile devices suggests that those circumstances may have been carefully calibrated to make it more difficult for such information to be surreptitiously intercepted. [REDACTED]

[REDACTED]

[REDACTED] However, given [REDACTED] evidence that [REDACTED], I do not consider the inference drawn by the *Amici* on this point to be strong.

[181] In any event, I am satisfied that the information from the *Gone Opaque* report and Wikipedia discussed above provides some support for the view that individuals’ subjective expectation of privacy in the IMSI and IMEI identifiers associated with their mobile devices is objectively reasonable.

Is the Use of CSS Technology Objectively Unreasonable?

[182] The *Amici* submit that CSS equipment is intrusive technology for which CSIS requires a warrant to operate. In this regard, the *Amici* rely on the following passage in *X (Re)*, above, at paras 161–162:

[161] When conventional means of investigation do not allow to meaningfully advance an investigation, sections 21(1), 21(2), and specifically 21(2)b) [further referred to simply as “section 21”] come into play to allow the CSIS to apply for warrants before the Court. The application must show, on reasonable grounds, that the information sought is factually related to a threat to the security of Canada as referred to in sections 21(1), 12(1), and as defined in section 2. The affidavit in support of the warrant application and the examination that follows at the hearing are determinative for the designated judge charged with deciding whether to issue the warrant or not. As the Pitfield Report rightly noted when discussing this primary function, the definition of the threats to the security of Canada at section 2 of the Act:

“[...] constitutes the basic limit on the agency’s freedom of action. It will establish for the CSIS, its director, and employees the fundamental standard for their activities. It will enter crucially into judicial determination of whether a particular intrusive investigative technique can be used.”
[Emphasis added.]

Senate of Canada, Special Committee of the Senate on the Canadian Security Intelligence Service, *Delicate Balance: A Security Intelligence Service in a Democratic Society*, (November 1983) (Chair: P.M Pitfield) at p 12, para 31.)

[162] Section 21 supports advancing an investigation when conventional means are not sufficient and intrusive methods are necessary. The role of the Court, in such cases, is to ensure all requirements of the legislation are respected in the application for warrants and that the measures sought are justified in light of the facts put forward. Section 21 does not create a separate scheme wholly distinct from the primary function of CSIS as described in section 12(1); rather, section 21 complements the primary function

of “investigating threats” by establishing procedural requirements when an application for warrants is sought.

(Emphasis in original)

[183] I do not read the foregoing passage as suggesting that CSIS requires a warrant whenever it wishes to gather information through the use of new technology. Indeed, the underlined words in the passage from the Pitfield Report that Justice Noël quoted specifically refer to a particular intrusive technique.

[184] In *Tessling*, above, at para 30, the Supreme Court made it clear that there is no “free-standing prohibition on [the use of] electronic or other technologies without a warrant.”

(See also, *Kang-Brown*, above, at para 54, and *Gomboc*, above, at para 40.) Rather, the question is: does the technology “in fact intrude on the reasonable sphere of privacy of an individual?”

The answer to this question requires an assessment of the “totality of the relevant circumstances.” In that assessment, in this particular case, I do not consider that there is anything about the use of CSS technology *per se* that would justify a conclusion that the use of that technology is objectively unreasonable.

Conclusion Regarding the Objective Reasonableness of Individuals’ Subjective Expectations of Privacy in Relation to the IMSI and IMEI Identifiers of their Mobile Devices

[185] In my view, a purposive consideration of the foregoing factors leads to the conclusion that individuals’ subjective expectations of privacy in relation to the IMSI and IMEI information on their mobile devices are objectively reasonable.

[186] The principal factors that support this conclusion include:

- i. The fact that information pertaining to one's mobile telecommunication devices and their use is generally considered to be very personal and private in nature. This includes information that could well be revealed through CSIS's analysis of IMSI and IMEI identifiers, which could assist CSIS to build a profile on the individual in question by (i) "determining [contacts] and communications patterns,"

[REDACTED]

[REDACTED] (ii) drawing inferences about an individual [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Even though CSIS may not know the identity of the individual whose IMSI and IMEI information is obtained through the use of CSS technology, these are not trivial encroachments on that individual's anonymity interests. In a thriving democratic society, it is objectively reasonable that individuals would likely expect that this personal information would remain private, and not be surreptitiously captured by the state.

- ii. The nature of the potentially serious consequences that may be faced by individuals who are subjects of investigation or information gathering under the Act.
- iii. The nature of the conduct addressed by section 12 of the Act—which is frequently closer to "true" crimes than to the types of regulatory offences established by the public welfare,

regulatory and economic legislation that has been considered in the jurisprudence with respect to section 8 of the *Charter*.

- iv. The fact that if the average person were aware that mobile devices emitted IMSI and IMEI identifiers to the cellular environment when they are in idle mode, he or she would likely believe that such information is being made available only to TSP.
- v. The information in the *Gone Opaque* report, and available on Wikipedia, which suggests that some steps have been taken in at least some quarters of the telecommunications industry to protect the confidentiality of IMSI numbers.

(v) Conclusion Regarding Whether the Capture of IMSI and IMEI Identifiers Constitutes a “Search.”

[187] Based on all of the foregoing, I conclude that CSIS’s capture of the IMSI and IMEI identifiers associated with ██████████ mobile devices through the use of CSS technology constituted a “search” within the meaning of section 8 of the *Charter*. In my view, this conclusion is supported by the confidential nature of IMSI and IMEI identifiers, the private and personal nature of the additional information that CSIS may be able to assemble upon obtaining IMSI and IMEI identifiers, the direct nature of ██████████ interest in that information, the subjective expectation of privacy that ██████████ likely had in respect of that information, and the objective reasonableness of that subjective expectation.

[188] It bears underscoring that, in a thriving democratic society, it is objectively reasonable that individuals would likely expect that the personal information that may be revealed to CSIS

once it begins to analyze captured IMSI and IMEI identifiers will remain private, and will not become known to agents of the state.

[189] Although intrusions on individuals' anonymity interests do not always engage section 8 of the *Charter*, I find that the capture of IMSI and IMEI information does reach this threshold, because of the profiles of individuals that CSIS can begin to build upon acquiring that information. Among other things, those technical and personal profiles can assist CSIS to construct a mosaic that reveals who an individual associates with, [REDACTED] [REDACTED] draw inferences regarding the person's beliefs. As I have previously noted, it is those very profiles that may ultimately assist CSIS to obtain a warrant to acquire subscriber information and engage in even more intrusive activities. However, until CSIS is able to obtain that subscriber data and exercise other warranted powers, its capture of IMSI and IMEI identifiers is only minimally intrusive. This is because neither the mobile device nor its contents, nor anything that might be accessed through the mobile device, can be accessed in any way through CSIS's CSS operations. Moreover, with the one exception of [REDACTED] CSIS cannot access the content of communications made on mobile devices; and CSIS has assured the Court that it does not use its CSS equipment to access such content.

(b) *Is CSIS's Interception of IMSI and IMEI Numbers Unreasonable?*

[190] Given that CSIS's capture of the IMSI and IMEI numbers from [REDACTED] mobile devices constituted a search, and given that CSIS's searches were conducted without a warrant,

they were presumptively unreasonable (*Spencer*, above, at para 68; *Goodwin*, above, at para 56; *Hunter*, above, at 160-161).

[191] To overcome that presumption, and in the absence of any suggestion that it was not feasible to seek a warrant before CSIS used CSS technology to capture the IMSI and IMEI identifiers associated with [REDACTED] mobile devices, the Attorney General must demonstrate that the “searches” were authorized by law, that the law in question is reasonable, and that the manner in which the searches was carried out was reasonable (see jurisprudence cited at paragraph 133 above). These issues will be addressed below.

(i) Was the “Search” Authorized by Law?

[192] The Attorney General submits that CSIS’s use of CSS technology to capture IMSI and IMEI numbers, without a warrant, for the purpose of identifying a subject of investigation’s mobile electronic device(s) is authorized by section 12 of the Act. As has been noted, that provision states as follows:

<i>Canadian Security Intelligence Service Act, RSC 1985, c C-23</i>	<i>Loi sur le Service canadien du renseignement de sécurité, LRC (1985), ch C-23</i>
Collection, analysis and retention	Informations et renseignements
12 (1) The Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on	12 (1) Le Service recueille, au moyen d’enquêtes ou autrement, dans la mesure strictement nécessaire, et analyse et conserve les informations et renseignements sur les

reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada.

activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada; il en fait rapport au gouvernement du Canada et le conseille à cet égard.

No territorial limit

Aucune limite territoriale

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

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

[193] The *Amici* disagree with that assertion for several reasons, some of which I will discuss in the next section below, when I address whether the framework established by sections 12 and 21 of the Act can be considered to be a “reasonable law” for the present purposes.

[194] The *Amici* state that section 12 is not a freestanding power to search once section 8 of the *Charter* has been engaged. They maintain that this would be inconsistent with the words of sections 12 and 21, when “read in their entire context and in their grammatical and ordinary sense harmoniously with the scheme of the Act, the object of the Act, and the intention of Parliament” (*Canada Trustco Mortgage Co v Canada*, 2005 SCC 54, at para 10). More specifically, they assert that section 12 simply identifies CSIS’s duties and functions and does not confer on CSIS the power to conduct searches that engage section 8 of the *Charter*. In this regard, they draw an analogy to the policing context, where the police have a duty to investigate crime, but do not have an unfettered power to search. The *Amici* maintain that the power to

search must be granted by statute or by the common law. However, this begs the question of whether section 12 confers such a power.

[195] The *Amici* submit that interpreting section 12 as conferring powers on CSIS personnel to conduct a search when section 8 of the *Charter* has been engaged is inconsistent with the manner in which this Court has previously interpreted section 12 of the Act. In this regard, they note that in *X (Re)*, above, Justice Noël observed that “[w]hen conventional means of investigation do not allow [CSIS] to meaningfully advance an investigation, sections 21(1), 21(2) and specifically 21(2)b [...] come into play to allow CSIS to apply for warrants before the Court” (*X (Re)*, above, at para 161). As discussed above at paragraphs 182-183, I do not interpret Justice Noël’s use of the term “conventional means of investigation” as suggesting that a warrant is required any time any new technology that cannot be characterized as “conventional” is used by CSIS. This would be contrary to the express teaching of the Supreme Court in *Tessling*, above, at para 30; and in *Kang-Brown*, above, at para 54.

[196] The plain language of section 12 requires CSIS to collect, by investigation or otherwise, to the extent that it is strictly necessary, and to analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada. This provides CSIS with the explicit authority to investigate such threats in those circumstances.

[197] The provisions in section 21, while linked to sections 12 and 16, simply describe the circumstances in which a warrant may be sought and issued, when (i) the Director of CSIS or

any employee designated by the Minister for the purpose, believes, on reasonable grounds, that a warrant is required to enable CSIS to investigate a threat to the security of Canada, or to perform the duties and functions set forth in section 16 of the Act, and (ii) a judge of this Court is satisfied of that fact, and of the matters described in paragraph 21(2)(a) and (b) (*Mahjoub v Canada (Citizenship and Immigration)*, 2017 FCA 157, at para 178 [*Mahjoub FCA*]). It is implicit that such belief on the part of the Director or a Minister's designate, and such determination by this Court, would be informed by the requirements of the common law as to when warrants are required for those purposes.

[198] In my view, there is nothing in the language of section 21, or elsewhere in the Act, that would support the view that CSIS is required to obtain a warrant anytime that it engages in a minimally intrusive "search" within the meaning of the *Charter*. The language of section 12, as limited in the manner discussed at paragraphs 212-216 below, provides CSIS with all the authority it requires to investigate activities that may on reasonable grounds be suspected of constituting threats to the security of Canada, without a warrant, unless a warrant is required at common law.

[199] The view that CSIS requires a warrant every time that a person's reasonable expectation of privacy is engaged would conflate the two elements in section 8 of the *Charter* into a single element, by effectively reading out the requirement that a search be "unreasonable" before it may be found to be contrary to section 8.

[200] The *Amici* further suggest that requiring a warrant before seeking to obtain IMSI and IMEI identifiers through the use of CSS technology would be consistent with the implicit requirement that the police must obtain a general warrant under section 487.01 of the *Criminal Code*, or a transmission data recorder warrant under section 492.2, before they may use a CSS to obtain and attribute IMSI and IMEI numbers to a suspect. However, the fact that Parliament *may* have determined that *police* require a warrant to use a CSS to attribute IMSI and IMEI numbers to an individual would not provide a sufficient basis for inferring that CSIS is also required to obtain a warrant in such circumstances. Among other things, police do not have available to them the powers conferred by section 12 of the Act.

[201] The *Amici* also maintain that it is for Parliament to decide whether to allow CSIS to use a CSS to intercept and attribute the IMSI and IMEI numbers of a mobile device to a subject of investigation, based on “reasonable grounds to suspect.” I agree, and I find that Parliament implicitly did so when it passed section 12 of the *Act*. Therefore, CSIS’s use of a CSS for that particular purpose is “authorized by law,” as contemplated by the jurisprudence cited at paragraph 133 above.

(ii) Is Section 12 of the Act a Reasonable Law?

[202] As discussed at paragraph 134 above, the factors to be considered in assessing whether a law which authorizes a search is reasonable include the nature and purpose of the law, the degree of intrusiveness that it authorizes, the mechanism of intrusion authorized, the extent to which it provides for judicial supervision, and any other safeguards or “checks and balances” that it contains to constrain the extent of the state’s intrusion on individuals’ privacy interests.

Depending upon the circumstances and the legislative scheme, the availability of oversight may assist to overcome the presumptive unlawfulness of a warrantless search. These factors will be addressed below.

The Nature and Purpose of Section 12

[203] Section 12 gives CSIS a critical, central and arguably essential role in Canada's national security apparatus. It does this by *requiring* CSIS to collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada, and in relation thereto, to report to and advise the Government of Canada.

[204] The *Amici* maintain that the "reasonable grounds to suspect" standard set forth in section 12 is not sufficient to justify a warrantless search by CSIS. I disagree.

[205] The Supreme Court explicitly recognized very early on in its consideration of section 8 of the *Charter* that the "reasonable grounds to believe" standard may not be required "where state security is involved" (*Hunter*, above, at 167-168).

[206] The Court has subsequently reiterated that the "balancing of interests can justify searches on a lower standard where privacy interests are reduced, or where state objectives of public importance are predominant" (*Chehil*, above, at para 23). In brief, the standard required to withstand scrutiny under section 8 "may vary depending on the context" (*Rodgers*, above, at para 35).

[207] In addition to circumstances in which privacy interests are reduced or state objectives of public importance are predominant, the Supreme Court has recognized that a standard that is lower than “reasonable grounds to believe” may be justified where the search method is highly accurate (*Goodwin*, above, at para 67), particularly where the search is minimally intrusive and narrowly targeted (*AM*, above, at paras 13, 42; *Kang-Brown*, above, at paras 25, 60, 210, 213).

[208] In each of *Chehil*, *AM* and *Kang-Brown*, above, the Supreme Court found that the “reasonable grounds to suspect” standard did not contravene section 8, notwithstanding the absence of judicial pre-authorization. The Court reached similar findings in respect of customs searches (*R v Simmons*, [1988] 2 SCR 495, at 527–529 [*Simmons*]; *R v Monney*, [1999] 1 SCR 652, at paras 37, 48) and a search for drugs on a student in a high school by a vice-principal (*R v M (MR)*, [1998] 3 SCR 393, at para 50).

[209] Applying the foregoing to CSIS’s use of CSS technology to intercept the IMSI and IMEI identifiers of [REDACTED] mobile electronic devices, each of the factors identified above is present. That is to say, state objectives of public importance (i.e., national security) are predominant, the intrusive nature of the search was minimal, and the method of the search was both highly accurate and narrowly targeted, given that the IMSI and IMEI information that was captured from third parties was not used for any purpose, and was quickly destroyed.

[210] Accordingly, the fact that section 12 authorized CSIS to engage in that minimally intrusive search of [REDACTED] mobile devices on a “reasonable grounds to suspect” standard, and

without prior judicial authorization, does not, in and of itself, render either section 12 or the search unreasonable (*Mahjoub FCA*, above, at paras 176-177).

[211] Indeed, I consider that the national security objectives permeating section 12 will generally be sufficient to tip the balance in favour of the state interest, when searches conducted by CSIS are minimally intrusive (*Jarvis*, above, at para 71; *Mahjoub FCA*, above). As the Supreme Court has recognized, “[o]ne of the most fundamental responsibilities of a government is to ensure the security of its citizens.” (*Charkaoui v Canada (Citizenship and Immigration)*, 2007 SCC 9, [2007] 1 SCR 350, at para 1). One need look no further than the recent terrorist attacks in Barcelona, London, Paris and Berlin, and the October 2014 attack on our very own Parliament, to appreciate why the interests of the state will generally predominate when the state’s interest in national security collides with an individual’s interest not to be subject to a minimally intrusive search. In such circumstances, the right to life, liberty and security of the person of individuals who may be in danger of serious harm (*Tse*, above, at para 21), namely, innocent victims of terrorist attacks, will typically prevail over the interests that are engaged when a minimally intrusive search is conducted by CSIS.

[212] Another factor that is important to consider in assessing the reasonableness of section 12 is whether it is overbroad or vague. The Attorney General submits that section 12 is neither, because it imposes objective standards and strict limits on the collection of information by CSIS. I agree.

[213] In particular, CSIS may collect, analyse and retain information for the purposes of an investigation, only in respect of activities that may on reasonable grounds be suspected of constituting “threats to the security of Canada.” The latter is defined in detail in section 2 of the Act, while the “reasonable grounds to suspect” requirement is a “robust” standard that is well known in Canadian law (*Chehil*, above, at paras 3, 26–37; *Kang-Brown*, above, at para 75). These objective parameters are further reinforced and narrowed by the fact that the scope of information that may be collected by CSIS is explicitly limited to that which “is strictly necessary.”

[214] In *X (Re)*, above, at para 185, Justice Noël found that this limitation also implicitly applies to the retention of information collected by CSIS. I consider it important to invoke judicial comity and follow Justice Noël’s position on this, without any further analysis, given the importance of consistency by this Court in respect of this very important issue. I will simply pause to note that neither the Attorney General nor the *Amici* took any issue with this interpretation of section 12 in this proceeding.

[215] Taken together, these limitations ensure that section 12 is neither overbroad nor vague and that the information collected by CSIS is rationally connected to the fulfillment of the mandate that section 12 has conferred upon CSIS. These limitations also ensure that section 12 “strikes the appropriate balance between the public interest in investigating threats to the security of Canada and [a subject of investigation’s] privacy rights” in respect of activities that are only minimally intrusive (*Mahjoub*, above, at para 35; *aff’d Mahjoub FCA*, above, at paras 176-177).

[216] In the presence of these clearly ascertainable and understandable limitations, it cannot be said that section 12 “so lacks in precision as not to give sufficient guidance for legal debate” (*R v Nova Scotia Pharmaceutical Society*, [1992] 2 SCR 606, at 643; *Wakeling*, above, at para 62). On the contrary, section 12, read together with the definition of “threats to the security of Canada” set forth in section 2 of the Act, clearly articulates the scope of activities that may be investigated by CSIS.

[217] Having regard to the foregoing, I find that the nature and purpose of section 12 support the view that section 12 is a reasonable law.

The Degree of Intrusiveness Authorized by Section 12

[218] The limitations discussed above ensure that CSIS does not have a mandate to engage in intrusive investigations in relation to persons whose activities fall outside of those limitations. In other words, CSIS has no mandate under section 12 to investigate persons whose activities do not give rise to reasonable grounds to suspect that they constitute threats to the security of Canada. The investigative powers provided to it under section 12 are confined to those whose activities meet this robust threshold, and then are further confined to the collection of information that “is strictly necessary,” as well as to the four categories of activities articulated in the definition of “threats to the security of Canada” provided in section 2 of the Act.

[219] For the narrowly circumscribed scope of remaining activities that fall within the purview of section 12, CSIS may collect, analyse and retain information that ranges from non-intrusive to highly intrusive. However, once it moves beyond minimally invasive collection activities, it will

require a warrant. In brief, by including the provisions of section 21 pertaining to warrants in the Act, Parliament implicitly contemplated that CSIS would not conduct collection activities under section 12 that are more than minimally intrusive, without first obtaining judicial pre-authorization under section 21. It can be inferred from this framework that, in the absence of a warrant, section 12 only provides CSIS with the ability to engage in non-intrusive or minimally intrusive activities.

The Extent to Which the Act Provides for Judicial Supervision

[220] The *Amici* submit that section 12 is not a reasonable law because it does not fall within any of the few exceptions that have been recognized to the general requirement that searches by agents of the state must be judicially pre-authorized on a standard of “reasonable grounds to believe.” In this regard, they assert that exceptions to the requirement of judicial pre-authorization have only been recognized in exigent circumstances (e.g., *R v Grant*, [1993] 3 SCR 223, at 243), the customs context (e.g., *Simmons*, above, at 528), “sniffer dog” searches (e.g., *Kang-Brown*, above, at para 60) and searches incident to detention and arrest (e.g., *R v Mann*, 2004 SCC 52, at paras 38–40).

[221] The *Amici* maintain that in each of these cases, the existence of after-the-fact judicial control was an important factor in the absence of judicial pre-authorization of the search. They add that no after-the-fact method of judicial control exists in respect of either warrantless or warranted searches under section 21 of the Act, because the individual who was the subject of the search may never learn that the search occurred.

[222] In my view, the Supreme Court's teachings in respect of judicial supervision of warrantless searches are more nuanced than suggested by the *Amici*.

[223] The jurisprudence relied upon by the *Amici* does not support the proposition that a minimally invasive search necessarily contravenes section 8 of the *Charter* in the absence of prior judicial authorization or after-the-fact judicial control. As I have already discussed the absence of prior judicial authorization at paragraphs 207-210 above, I will confine the discussion below to after-the-fact judicial control.

[224] The Supreme Court has consistently maintained that assessment of a warrantless search under section 8 will depend on a careful balancing of the legitimate interests of the state and the legitimate interests of the person who was the subject of a warrantless search in each particular case (*Kang-Brown*, above, at para 24; *AM*, above, at para 37; *Rodgers*, above, at paras 26–27; *Jarvis*, above, at paras 61–62; *Colarusso*, above, at 52–53; *McKinlay*, above, at 645-646). This balancing must be conducted as part of the overall assessment of whether the search was authorized by law, the law in question is reasonable, and the manner in which the search was carried out was reasonable.

[225] In a trilogy of “sniffer dog” cases (*Kang-Brown*, *AM* and *Chehil*, above) the Supreme Court placed considerable importance on the availability of after-the-fact judicial review of the warrantless searches that were conducted, in assessing the overall reasonableness of those searches. However, that appears to have been in part because of concerns regarding the reliability of individual dogs (*Chehil*, above, at paras 25, 48–54; *AM*, above, at paras 84–86, 90), in part

because of “the significance and quality of the information obtained about” the concealed contents of a person’s belongings or “on his [...] person” (*Kang-Brown*, above, at para 58), and in part because “the consequences of a false indication by a sniffer dog can be severe” (*Chehil*, above, at para 49).

[226] Those cases can be distinguished from CSIS’s use of CSS technology to capture IMSI and IMEI numbers from an individual’s wireless electronic devices. This is because that technology is highly reliable and therefore does not give rise to the potentially severe consequences associated with a “false positive.” Moreover, it intrudes far less on an individual’s privacy rights than a dog sniff, which can give rise to strong inferences about the concealed *contents* of an individual’s luggage, handbag or backpack, etc., or about what is on a person. In brief, IMSI and IMEI information cannot give rise to any inferences whatsoever about the *contents* stored on, or available through, a mobile device. IMSI and IMEI identifiers also cannot assist CSIS to make strong inferences about the specific content of communications made over a mobile device.

[227] The highly reliable nature of CSS technology, and the degree to which it intrudes on an individual’s privacy interests, also distinguishes this case from *Goodwin*, above, at para 72, where the Court considered the unavailability of after-the-fact judicial review of a licence suspension following a Breathalyzer search to be critical, “particularly given the concerns about the reliability of the [Breathalyzer device], the lack of an intermediate step between the [Breathalyzer analysis] and the roadside suspension, and the immediacy of the penalties that ensue.”

[228] In the particular circumstances of this case, I consider the nature of the state's interest (national security) to be sufficiently important that the absence of any requirement in the Act for a post-judicial review of each and every intercept of IMSI and IMEI identifiers by CSIS does not render section 12 unreasonable. This is especially so because of the minimal nature of CSIS's intrusion on an individual's privacy interests, the fact that such minimal intrusions are authorized by law (i.e., section 12), the fact that section 12 contains the various limitations discussed at paragraphs 212-216 above, the additional checks and balances that I will discuss below, and the fact that a warrant from this Court will be required [REDACTED]

[REDACTED]

At the time that CSIS seeks such a warrant, the Court would have an opportunity to review the reasonableness of CSIS's grounds to suspect that the individual's activities may constitute threats to the security of Canada. Prior to that time, the potential consequences of the search to the individual would be very limited, if any.

[229] I recognize that this after-the-fact judicial control under the Act is only available where CSIS decides to seek warranted powers in respect of the subject of investigation. According to

[REDACTED]

[REDACTED] The IMSI and IMEI numbers subsequently captured are then used to assist CSIS to execute the warranted powers against the correct wireless device. However, where a warrant has not been obtained prior to a CSS operation, there may be no opportunity for any judicial control in respect of any minimal intrusions that may occur in relation to the privacy rights of (i) subjects of investigation who do not become the subject of requests for warrants, or (ii) third parties.

Nevertheless, this is broadly analogous to the situation that exists in the sniffer dog cases

discussed above. In those cases, after-the-fact judicial control would only be available if criminal proceedings were instituted against an individual whose person or luggage, etc., had been subjected to a sniffer dog search (*Chehil*, above, at para 53; *AM*, above, at para 90; *Kang-Brown*, above, at para 59). Thus, the absence of some form of after-the-fact judicial control in respect of *all* minimally-invasive searches that may be conducted under a law does not, in and of itself, appear to render that law unreasonable.

The Presence of Other “Checks and Balances” or Accountability Measures

[230] In addition to the after-the-fact judicial review that the Act contemplates will occur if CSIS wishes to link IMSI and IMEI numbers that it has captured from an individual’s mobile devices to the specific personal identity of that person, the Act provides for a number of other accountability measures or “checks and balances.”

[231] Specifically, subsection 6(1) stipulates that the Director of CSIS is “under the direction of the Minister” in exercising his control and management of CSIS and all matters connected therewith. Furthermore, subsection 6(2) stipulates that the Minister may issue written directions to the Director. The Attorney General notes that one such direction, entitled “Ministerial Direction for Operations and Accountability,” states that CSIS’s “[o]perational activities must be reasonable and proportional to the threat” and that it “shall seek to minimize intrusions on human rights, including privacy, to the extent possible and in accordance with Canadian law”. Also, subsection 6(4) requires the Director of CSIS to provide an annual report to the Minister with respect to its operational activities during the year. I consider it appropriate to take judicial notice

of recent public statements made by the current Minister that indicate that he takes his role under section 6 of the Act very seriously.

[232] In addition, pursuant to subsection 20(2), the Director of CSIS is required to report to the Minister where he is of the opinion that an employee may, on a particular occasion, have acted unlawfully in the purported performance of CSIS's duties and functions under the Act. I note in passing that such reports are also required to be provided to the Attorney General (subsection 20(3)).

[233] Moreover, CSIS's activities are subject to review by the Security Intelligence Review Committee [SIRC], which was established pursuant to subsection 34(1) of the Act. The extensive functions of the SIRC are set forth in subsection 38(1), and include generally reviewing the performance by CSIS of its duties and functions. Pursuant to subsection 20(4), a copy of any report prepared by the Director under subsection 20(2) and provided to the Attorney General under subsection 20(3) must also be given to the SIRC, which is then mandated by paragraph 38(1)(a)(iv) to review that report. SIRC is also mandated to submit a certificate to the Minister stating the extent to which it is satisfied with CSIS's annual report and stating whether, in its opinion, any of CSIS's activities described in that report (i) are not authorized by or under the Act or contravene any directions issued by the Minister under subsection 6(2), or (ii) involve an unreasonable or unnecessary exercise by CSIS of any of its powers.

[234] As noted at paragraph 11 of these reasons above, the Court first learned of the existence of CSIS's use of CSS technology when it was provided with a copy of one of SIRC's classified

reports. As with SIRC's revelation (in that same report) of CSIS's use of metadata, this appears to have led, at least in part, to CSIS becoming more transparent with this Court about its use of CSS technology. I consider SIRC's oversight of CSIS's activities in respect of metadata and CSS technology to have been essential in this regard.

[235] In my view, the roles and responsibilities of the Minister, SIRC and CSIS's Director described above assist in ensuring that section 12 is a reasonable law for the purposes of assessing whether the minimally invasive searches that it authorizes are reasonable.

Conclusion Regarding the Reasonableness of Section 12

[236] Based on the foregoing assessment in Part VII.C.2.(b)(ii) immediately above, I conclude that section 12 is a reasonable law. In my view, this conclusion is supported by the following:

- i. *Nature and purpose of section 12*: Section 12 gives CSIS a critical, central and arguably essential role in Canada's national security apparatus. Parliament's objective in conferring this role upon CSIS is of predominant importance, relative to the minimal intrusions that are authorized under section 12 (*Chehil*, above, at para 23; *Tse*, above, at para 21). In this context, the "reasonable grounds to suspect" standard, together with the absence of judicial pre-authorization, are justified, particularly where (i) the minimal intrusion on an individual's right to privacy is as narrowly targeted and as highly accurate as CSIS's use of CSS technology, and (ii) CSIS destroys the IMSI and IMEI information incidentally captured from third parties very quickly, without conducting any analysis of that information

whatsoever, once it has been confirmed that it does not come from a wireless device owned or operated by a subject of investigation. The limitations contained in section 12, and in the definition of “threat to the security of Canada” that is set forth in section 2 of the Act, ensure that section 12 is neither overbroad nor vague and that the information collected by CSIS is rationally connected to the fulfillment of the mandate that section 12 has conferred upon CSIS.

- ii. *Degree of intrusiveness authorized by section 12:* The limitations described above ensure that CSIS does not have a mandate to engage in intrusive investigations in relation to persons whose activities fall outside of those limitations. For the narrowly circumscribed scope of remaining activities, CSIS may collect, analyse and retain information that ranges from non-intrusive to highly intrusive. However, the provisions in section 21 of the Act pertaining to warrants contemplate that CSIS may not engage in activities that are more than minimally intrusive without a warrant.
- iii. *Extent to which the Act provides for judicial supervision:* The judicial supervision contemplated in the provisions of section 21 of the Act would be triggered as soon as CSIS seeks powers to engage in investigative activities against an individual that are more than minimally-intrusive in nature. Such activities would include obtaining subscriber information in respect of the mobile devices that have been attributed to an individual pursuant to a CSS operation. At that time, the Court would have an opportunity to evaluate, among other things, the reasonableness of the grounds to suspect that the individual’s activities may constitute threats to the

security of Canada. Such after-the-fact judicial control is broadly analogous to the judicial scrutiny that is triggered in other contexts, and only after criminal proceedings have been initiated against the individual whose privacy rights were intruded upon.

- iv. The Act contemplates a meaningful oversight role for SIRC, which SIRC has provided. In addition, the Act stipulates that the Director of CSIS is “under the direction of the Minister” in exercising his control and management of CSIS and all matters connected therewith. The Director is also subject to a number of reporting obligations to the Minister, including providing an annual report that is tabled in Parliament. Moreover, the Minister has the authority to issue written directions to the Director, and one such direction that has been issued imposes significant constraints on the Director, which extend beyond those that are contained in section 12.

(iii) Was the Manner in Which the Search was Carried Out Unreasonable?

[237] The bulk of the evidence adduced in this proceeding regarding the manner in which CSS operations are conducted relates to CSS operations generally, rather than to the specific CSS operation that was conducted in respect of [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[238] In addition, the IMSI and IMEI information that was captured from third parties at the time of CSIS's CSS operations against [REDACTED] devices was destroyed before any analysis was performed in respect of that information; and that information was not included in the report that was prepared by CSIS in respect of the CSS operations in question. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] In view of the fact that I am addressing various issues relating to those types of powers in [REDACTED] which is being released contemporaneously with this decision, I will refrain from commenting upon the issue further here.

[239] With respect to CSIS's CSS operations generally, the evidence adduced in this proceeding is more extensive. In particular, [REDACTED] testified that CSIS's equipment maintains contact with mobile devices [for a few seconds] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Based on the fact that an average telephone call from a mobile device typically takes approximately five to 15 seconds to go through, and will persist in trying to connect a call for "up to tens of seconds," [REDACTED] has testified that CSS operations have no discernible adverse impact on the experience of a user of a

mobile device. For greater certainty, [REDACTED] testified that CSIS's CSS equipment does not cause active calls to be dropped.

[240] In addition, CSIS's CSS operations do not impact upon the ability of mobile device users to place a 911 call, because the first legitimate network in any given area that receives such a call will connect it, even if that tower is operated by a TSP with which the mobile user does not have a relationship.

[241] Furthermore, with one exception, the CSS equipment operated by CSIS does not have the ability to intercept the content of any communications, or to obtain any information stored in a mobile device. [REDACTED]

[REDACTED] testified that CSIS has a policy of not capturing such content.

[242] Finally, [REDACTED] testified that CSIS deletes the IMSI and IMEI information that it captures from the mobile devices of third parties very quickly, often within [REDACTED] days, and in any event as soon as an operational report has been written with respect to a particular CSS operation or set of operations. Moreover, once it is concluded that such IMSI and IMEI information does not relate to the mobile devices that are the focus of a CSS operation, [REDACTED]

[REDACTED] no analysis whatsoever is conducted in respect of that information.

[243] Having regard to the all of foregoing, I am satisfied that the manner in which CSIS's CSS operations are presently conducted is not unreasonable.

- (iv) Conclusion regarding the reasonableness of CSIS's use of CSS technology

[244] For the reasons summarized at the end of Parts VII.C.(2)(b)(i)-(iii) above, I have found that CSIS's use of CSS technology to capture IMSI and IMEI identifiers from the mobile device(s) of a subject of investigation is authorized by section 12 of the Act, that section 12 is a reasonable law, and that the manner in which CSIS currently conducts its CSS operations is not unreasonable. In reaching these findings, I have been mindful of the need to adopt "a purposive approach that emphasizes the protection of privacy as a prerequisite to individual security, self-fulfilment and autonomy as well as to the maintenance of a thriving democratic society" (*Spencer*, above, at para 15).

[245] Based on those findings, I conclude that this activity, as currently conducted by CSIS, is not unreasonable. In other words, I concur with SIRC's finding that CSIS does not require a warrant to engage in this activity, provided that it is conducted in the manner described in my reasons above. I note that although the *Amici* came to a contrary conclusion, they observed that this activity was "just over the threshold" at which a warrant would be required. They added that the contrary conclusion could also reasonably be reached.

[246] This conclusion rests largely on the particular evidence adduced in this proceeding, regarding the manner in which CSIS currently conducts its CSS operations, and regarding the current capabilities of CSIS's CSS equipment. I expect that the measures I have identified in concluding that CSIS's capture of IMSI and IMEI identifiers is minimally intrusive, and

therefore lawful, will be scrutinized by both the Minister and by SIRC, in their future consideration of CSIS's use of CSS technology.

VIII. Conclusion

[247] For the reasons that I have set forth above, CSIS's use of CSS technology to capture IMSI and IMEI identifiers from [REDACTED] wireless devices, without a warrant, engaged section 8 of the *Charter* because that activity constituted a "search." This is because it assisted CSIS to build a profile on him, including by helping CSIS to begin to "determine his [REDACTED] [contacts] and communications patterns," with the aid of information already available to CSIS. This engaged [REDACTED] rights under section 8 of the *Charter*, because it de-anonymized his use of his wireless devices, which are very personal in nature.

[248] However, that activity was not "unreasonable," as contemplated by section 8. Therefore, it was not unlawful.

[249] This is because the "searches" were narrowly targeted, highly accurate and minimally-intrusive, largely due to measures that CSIS implements when conducting its CSS operations. If those measures had not been adopted by CSIS, I may well have reached a different conclusion.

[250] More particularly, the searches were not unreasonable because neither the mobile devices nor their contents, nor anything that might be accessed through the mobile devices, could be accessed in any way by CSIS's CSS equipment. Moreover, with the one exception [REDACTED] [REDACTED] that equipment cannot access the content of

communications made on mobile devices. CSIS has assured the Court that it does not use its CSS equipment to access such content.

[251] In addition, CSIS's equipment maintains contact with mobile devices [REDACTED]

[for a few seconds] [REDACTED] Based on the fact that an average telephone call from a mobile device typically takes approximately five to 15 seconds to go through, and will persist in trying to connect a call for "up to tens of seconds," the uncontested evidence is that CSIS's CSS operations have no discernible adverse impact on the experience of a user of a mobile device. Moreover, CSIS's CSS operations do not impact upon the ability of mobile device users to place a 911 call, because the first legitimate network in any given area that receives such a call will connect it, even if that tower is operated by a TSP with which the mobile user does not have a relationship.

[252] Finally, CSIS deletes the IMSI and IMEI information that it captures from the mobile devices of third parties very quickly, often within [REDACTED] days, and in any event as soon as an operational report has been written with respect to a particular CSS operation or set of operations. Moreover, once it is concluded that such IMSI and IMEI information does not relate to the mobile devices that are the focus of a CSS operation, [REDACTED]

[REDACTED] no analysis whatsoever is performed in respect of that information.

[253] In my view, the expeditious destruction of third party IMSI and IMEI information, together with CSIS's policy of performing no further analysis in respect of such information, are essential to ensuring that a CSS operation is reasonable, and is not overbroad (*Chehil*, above,

[256] I will simply add three further concluding remarks.

[257] First, CSIS should not be relying on the language of [REDACTED] or on any other warrant, to conduct any CSS operations whatsoever. Should CSIS wish to obtain a warrant to conduct such operations, it should request explicit language authorizing it to do so.

[258] Second, where CSIS wishes to rely on any information that it has directly or indirectly obtained from a CSS operation, in any future applications that CSIS may make to the Court for warrants, it should ensure that the Court is informed of the following, relative to the evidence that was provided in this proceeding: (i) any changes to the manner in which it conducts CSS operations; (ii) any changes to the capabilities of the equipment that it uses in such operations; and (iii) any changes in the purposes for which such equipment is used.

[259] Finally, I consider that the use of CSS technology to conduct the “bulk” capture of the IMSI or IMEI identifiers associated with the mobile devices of members of the general public would not be authorized by section 12. Given the speculative nature of such an operation, it would therefore not meet the test for a warrantless search (*Kang-Brown*, above, at paras 26 and 75).

JUDGMENT in [REDACTED]

THIS COURT’S JUDGMENT is that CSIS’s warrantless use of CSS technology to capture the identifying characteristics of [REDACTED] mobile devices was not unlawful. It did not contravene the *Radiocommunication Act*, RSC 1985, c R-2, the *Criminal Code*, RSC 1985, c C-46 or section 8 of the *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act 1982 (UK)*, 1982, c 11. Although CSIS’s use of a CSS against [REDACTED] constituted a “search”, the search was not “unreasonable” because it was narrowly targeted, highly accurate and minimally intrusive.

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

“Paul S. Crampton”

Chief Justice

APPENDIX I

EXHIBIT "C"

AUTHORITY TO USE RADIO

- 1) In accordance with subparagraph 5(1)(a)(v) of the Radiocommunication Act, this constitutes authorization for the Canadian Security Intelligence Service (CSIS) in respect of any and all types of specially designed radio apparatus used for the purposes specified in paragraph 2, for which a radio licence, under subparagraph 5(1)(a)(i) of the Radiocommunication Act, is not appropriate.
- 2) This authorization applies to radio apparatus specified in paragraph 1 only when it is being tested, used for training, or used for operations, solely in relation to investigations under sections 12 and 16 of the Canadian Security Intelligence Service Act, R.S.C. 1985, c. C-23.
- 3) The radio apparatus specified in paragraph 1, used for the purpose specified in paragraph 2, is not subject to section 4(2) of the Radiocommunication Act which requires radio apparatus have a Departmental technical acceptance certificate.
- 4) The radio apparatus specified in paragraph 1, used for the purpose specified in paragraph 2, is not subject to section 4(3) of the Radiocommunication Act which requires radio apparatus comply with Departmental technical standards.
- 5) This authorization does not obviate the requirement to obtain a radio station licence or authority required for radio apparatus under the Radiocommunication Act for purposes not specified in paragraph 2.
- 6) This authorization does not apply to radio apparatus for which no licence is required, or for which a licence or authority has been obtained under the Radiocommunication Act.
- 7) All radio apparatus covered by this authorization shall not cause harmful interference to other authorized or licensed radio apparatus.
- 8) No protection is afforded to radio apparatus covered by this authorization from the effects of interference.
- 9) This authorization is valid unless withdrawn by the Department of Communications or the Canadian Security Intelligence Service (CSIS) indicates in writing that it is no longer required.

Original signed by /
Original signé par
Perrin Beatty

Perrin Beatty
Minister of Communications

Dated: SEP - 1 1992

S
E
C
R
E
T

S
E
C
R
E
T

APPENDIX II



Innovation, Science and
Economic Development Canada

Innovation, Sciences et
Développement économique Canada

Our File: 49081700428

MAR 13 2017

Mr. Peter Henschel
Deputy Commissioner
Specialized Policing Services
Royal Canadian Mounted Police
273 Leikin Drive
Ottawa, Ontario K1A 0R2

Mr. Henschel,

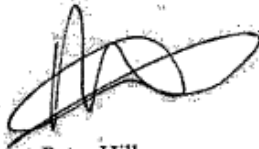
This letter constitutes an authorization issued under section 5(1)(a)(v) of the *Radiocommunication Act*, for employees of the Royal Canadian Mounted Police (RCMP) Technical Investigation Services Branch, as well as employees of the RCMP who fall under the direction of that Branch. This authorization applies only to the installation, operation and possession of radio apparatus designed to communicate with mobile devices on commercial mobile networks to obtain data associated with a mobile device or the mobile network that, as per section 492.2 of the *Criminal Code*:

- (a) relates to the telecommunication functions of dialing, routing, addressing or signalling;
- (b) is transmitted to identify, activate or configure a device, including a computer program as defined in subsection 342.1(2) of the *Criminal Code*, in order to establish or maintain access to a telecommunication service for the purpose of enabling a communication, or is generated during the creation, transmission or reception of a communication and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination or termination of the communication; and
- (c) does not reveal the substance, meaning or purpose of the communication.

..2/

This authorization is subject to the attached terms and conditions, and expires five years from the day it is signed. In particular, these radio apparatus may be installed, operated or possessed only in accordance with the purposes under section 54 of the *Radiocommunication Regulations*.

Yours Sincerely,

A handwritten signature in black ink, appearing to be 'Peter Hill', written in a cursive style.

Peter Hill
Director General
Spectrum Management Operations Branch

Attachment

APPENDIX III

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

Definitions

2 In this Act,

threats to the security of Canada means

(a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage,

(b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person,

(c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state, and

(d) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada,

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

[...]

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

Définitions

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

menaces envers la sécurité du Canada

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

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

b) les activités influencées par l'étranger qui touchent le Canada ou s'y déroulent et sont préjudiciables à ses intérêts, et qui sont d'une nature clandestine ou trompeuse ou comportent des menaces envers quiconque;

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

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

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

[...]

Management of Service

Role of Director

6 (1) The Director, under the direction of the Minister, has the control and management of the Service and all matters connected therewith.

Minister may issue directions

(2) In providing the direction referred to in subsection (1), the Minister may issue to the Director written directions with respect to the Service and a copy of any such direction shall, forthwith after it is issued, be given to the Review Committee.

Directions deemed not to be statutory instruments

(3) Directions issued by the Minister under subsection (2) shall be deemed not to be statutory instruments for the purposes of the *Statutory Instruments Act*.

Periodic reports by Director

(4) The Director shall, in relation to every 12-month period or any lesser period that is specified by the Minister, submit to the Minister, at any times that the Minister specifies, reports with respect to the Service's operational activities during that period, and shall cause the Review Committee to be given a copy of each such report.

Measures to reduce threats to the security of Canada

5) The reports shall include, among other things, the following information in respect of the Service's operational activities, during the period for which the report is made, to reduce threats to the security of Canada:

(a) for each of the paragraphs of the definition threats to the security of Canada in section 2, a

Gestion

Rôle du directeur

6 (1) Sous la direction du ministre, le directeur est chargé de la gestion du Service et de tout ce qui s'y rattache.

Instructions du ministre

(2) Dans l'exercice de son pouvoir de direction visé au paragraphe (1), le ministre peut donner par écrit au directeur des instructions concernant le Service; un exemplaire de celles-ci est transmis au comité de surveillance dès qu'elles sont données.

Non-application de la Loi sur les textes réglementaires

(3) Les instructions visées au paragraphe (2) sont réputées ne pas être des textes réglementaires au sens de la *Loi sur les textes réglementaires*.

Rapports périodiques

(4) Pour chaque période de douze mois d'activités opérationnelles du Service ou pour les périodes inférieures à douze mois et aux moments précisés par le ministre, le directeur présente à celui-ci des rapports sur ces activités; il en fait remettre un exemplaire au comité de surveillance.

Mesure pour réduire les menaces envers la sécurité du Canada

(5) Les rapports précisent notamment les éléments d'information ci-après au sujet des activités opérationnelles exercées par le Service durant la période visée pour réduire les menaces envers la sécurité du Canada :

a) pour chacun des alinéas de la définition de menaces envers la sécurité du Canada à l'article 2,

general description of the measures that were taken during the period in respect of the threat within the meaning of that paragraph and the number of those measures;

(b) the number of warrants issued under subsection 21.1(3) during the period and the number of applications for warrants made under subsection 21.1(1) that were refused during the period; and

(c) for each threat to the security of Canada for which warrants have been issued under subsection 21.1(3) before or during the period, a general description of the measures that were taken under the warrants during the period.

[...]

Duties and Functions of Service

Collection, analysis and retention

12 (1) The Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada.

No territorial limit

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

[...]

Collection of information concerning foreign states and persons

16 (1) Subject to this section, the Service may, in relation to the defence of Canada or the conduct of the international affairs of Canada, assist the

une description générale des mesures prises à l'égard des menaces au sens de l'alinéa en cause et le nombre de ces mesures;

b) le nombre de mandats décernés en vertu du paragraphe 21.1(3) et le nombre de demandes de mandat présentées au titre du paragraphe 21.1(1) qui ont été rejetées;

c) pour chacune des menaces envers la sécurité du Canada à l'égard desquelles des mandats ont été décernés en vertu du paragraphe 21.1(3) durant la période ou avant que celle-ci ne débute, une description générale des mesures prises en vertu des mandats en cause.

[...]

Fonctions du Service

Informations et renseignements

12 (1) Le Service recueille, au moyen d'enquêtes ou autrement, dans la mesure strictement nécessaire, et analyse et conserve les informations et renseignements sur les activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada; il en fait rapport au gouvernement du Canada et le conseille à cet égard.

Aucune limite territoriale

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

[...]

Assistance

16 (1) Sous réserve des autres dispositions du présent article, le Service peut, dans les domaines de la défense et de la conduite des affaires

Minister of National Defence or the Minister of Foreign Affairs, within Canada, in the collection of information or intelligence relating to the capabilities, intentions or activities of

internationales du Canada, prêter son assistance au ministre de la Défense nationale ou au ministre des Affaires étrangères, dans les limites du Canada, à la collecte d'informations ou de renseignements sur les moyens, les intentions ou les activités :

(a) any foreign state or group of foreign states; or

a) d'un État étranger ou d'un groupe d'États étrangers;

(b) any person other than

b) d'une personne qui n'appartient à aucune des catégories suivantes :

(i) a Canadian citizen,

(i) les citoyens canadiens,

(ii) a permanent resident within the meaning of subsection 2(1) of the *Immigration and Refugee Protection Act*, or

(ii) les résidents permanents au sens du paragraphe 2(1) de la *Loi sur l'immigration et la protection des réfugiés*,

(iii) a corporation incorporated by or under an Act of Parliament or of the legislature of a province.

(iii) les personnes morales constituées sous le régime d'une loi fédérale ou provinciale.

Limitation

Restriction

(2) The assistance provided pursuant to subsection (1) shall not be directed at any person referred to in subparagraph (1)(b)(i), (ii) or (iii).

(2) L'assistance autorisée au paragraphe (1) est subordonnée au fait qu'elle ne vise pas des personnes mentionnées à l'alinéa (1)b).

Personal consent of Ministers required

Consentement personnel des ministres

(3) The Service shall not perform its duties and functions under subsection (1) unless it does so

(3) L'exercice par le Service des fonctions visées au paragraphe (1) est subordonné :

(a) on the personal request in writing of the Minister of National Defence or the Minister of Foreign Affairs; and

a) à une demande personnelle écrite du ministre de la Défense nationale ou du ministre des Affaires étrangères;

(b) with the personal consent in writing of the Minister.

b) au consentement personnel écrit du ministre.

[...]

[...]

Judicial Control

Contrôle judiciaire

Application for warrant

Demande de mandat

21 (1) If the Director or any employee

21 (1) Le directeur ou un employé désigné à cette

designated by the Minister for the purpose believes, on reasonable grounds, that a warrant under this section is required to enable the Service to investigate, within or outside Canada, a threat to the security of Canada or to perform its duties and functions under section 16, the Director or employee may, after having obtained the Minister's approval, make an application in accordance with subsection (2) to a judge for a warrant under this section.

Matters to be specified in application for warrant

(2) An application to a judge under subsection (1) shall be made in writing and be accompanied by an affidavit of the applicant deposing to the following matters, namely,

(a) the facts relied on to justify the belief, on reasonable grounds, that a warrant under this section is required to enable the Service to investigate a threat to the security of Canada or to perform its duties and functions under section 16;

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

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

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

Contenu de la demande

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

a) les faits sur lesquels le demandeur s'appuie pour avoir des motifs raisonnables de croire que le mandat est nécessaire aux fins visées au paragraphe (1);

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

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

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

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

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

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

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

Issuance of warrant

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

(a) to enter any place or open or obtain access to any thing;

(b) to search for, remove or return, or examine, take extracts from or make copies of or record in any other manner the information, record, document or thing; or

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

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

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

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

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

Délivrance du mandat

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

a) l'accès à un lieu ou un objet ou l'ouverture d'un objet;

b) la recherche, l'enlèvement ou la remise en place de tout document ou objet, leur examen, le prélèvement des informations qui s'y trouvent, ainsi que leur enregistrement et l'établissement de copies ou d'extraits par tout procédé;

(c) to install, maintain or remove any thing.

c) l'installation, l'entretien et l'enlèvement d'objets.

Activities outside Canada

Activités à l'extérieur du Canada

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

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

Matters to be specified in warrant

Contenu du mandat

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

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

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

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

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

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

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

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

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

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

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

e) la durée de validité du mandat;

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

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

Maximum duration of warrant

Durée maximale

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

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

(a) sixty days where the warrant is issued to enable the Service to investigate a threat to the security of Canada within the meaning of paragraph (d) of the definition of that expression in section 2; or

(b) one year in any other case.

[...]

Security Intelligence Review Committee

Security Intelligence Review Committee

34 (1) There is hereby established a committee, to be known as the Security Intelligence Review Committee, consisting of a Chairman and not less than two and not more than four other members, all of whom shall be appointed by the Governor in Council from among members of the Queen's Privy Council for Canada who are not members of the Senate or the House of Commons, after consultation by the Prime Minister of Canada with the Leader of the Opposition in the House of Commons and the leader in the House of Commons of each party having at least twelve members in that House.

Term of office

(2) Each member of the Review Committee shall be appointed to hold office during good behaviour for a term not exceeding five years.

Re-appointment

3) A member of the Review Committee is eligible to be re-appointed for a term not exceeding five years.

Expenses

(4) Each member of the Review Committee is entitled to be paid, for each day that the member performs duties and functions under this Act, such remuneration as is fixed by the Governor in

a) de soixante jours, lorsque le mandat est décerné pour permettre au Service de faire enquête sur des menaces envers la sécurité du Canada au sens de l'alinéa d) de la définition de telles menaces contenue à l'article 2;

b) d'un an, dans tout autre cas.

[...]

Comité de surveillance des activités de renseignement de sécurité

Constitution du comité de surveillance

34 (1) Est constitué le comité de surveillance des activités de renseignement de sécurité, composé du président et de deux à quatre autres membres, tous nommés par le gouverneur en conseil parmi les membres du Conseil privé de la Reine pour le Canada qui ne font partie ni du Sénat ni de la Chambre des communes. Cette nomination est précédée de consultations entre le premier ministre du Canada, le chef de l'opposition à la Chambre des communes et le chef de chacun des partis qui y disposent d'au moins douze députés.

Durée du mandat

(2) Les membres du comité de surveillance sont nommés à titre inamovible pour une durée maximale de cinq ans.

Renouvellement

(3) Le mandat des membres du comité de surveillance est renouvelable pour une durée maximale identique.

Rémunération et frais

(4) Les membres du comité de surveillance ont le droit de recevoir, pour chaque jour qu'ils exercent les fonctions qui leur sont conférées en vertu de la présente loi, la rémunération que fixe le

Council and shall be paid reasonable travel and living expenses incurred by the member in the performance of those duties and functions.

[...]

Functions of Review Committee

38 (1) The functions of the Review Committee are

(a) to review generally the performance by the Service of its duties and functions and, in connection therewith,

(i) [Repealed, 2012, c. 19, s. 381]

(ii) to review directions issued by the Minister under subsection 6(2),

(iii) to review arrangements entered into by the Service pursuant to subsections 13(2) and (3) and 17(1) and to monitor the provision of information and intelligence pursuant to those arrangements,

(iv) to review any report or comment given to it pursuant to subsection 20(4),

(v) to monitor any request referred to in paragraph 16(3)(a) made to the Service,

(vi) to review the regulations, and

(vii) to compile and analyse statistics on the operational activities of the Service;

(b) to arrange for reviews to be conducted, or to conduct reviews, pursuant to section 40; and

(c) to conduct investigations in relation to

(i) complaints made to the Committee under sections 41 and 42,

(ii) reports made to the Committee pursuant to

gouverneur en conseil et sont indemnisés des frais de déplacement et de séjour entraînés par l'exercice de ces fonctions.

[...]

Fonctions du comité de surveillance

38 (1) Le comité de surveillance a les fonctions suivantes :

a) surveiller la façon dont le Service exerce ses fonctions et, à cet égard :

(i) [Abrogé, 2012, ch. 19, art. 381]

(ii) examiner les instructions que donne le ministre en vertu du paragraphe 6(2),

(iii) examiner les ententes conclues par le Service en vertu des paragraphes 13(2) et (3) et 17(1), et surveiller les informations ou renseignements qui sont transmis en vertu de celles-ci,

(iv) examiner les rapports et commentaires qui lui sont transmis en conformité avec le paragraphe 20(4),

v) surveiller les demandes qui sont présentées au Service en vertu de l'alinéa 16(3)a

(vi) examiner les règlements,

(vii) réunir et analyser des statistiques sur les activités opérationnelles du Service;

b) effectuer ou faire effectuer des recherches en vertu de l'article 40;

c) faire enquête sur :

(i) les plaintes qu'il reçoit en vertu des articles 41 et 42,

(ii) les rapports qui lui sont transmis en vertu de

section 19 of the *Citizenship Act*, and

(iii) matters referred to the Committee pursuant to section 45 of the *Canadian Human Rights Act*.

Review of measures

(1.1) In reviewing the performance by the Service of its duties and functions the Review Committee shall, each fiscal year, review at least one aspect of the Service's performance in taking measures to reduce threats to the security of Canada.

Review Committee's other functions

(2) As soon as the circumstances permit after receiving a copy of a report referred to in subsection 6(4), the Review Committee shall submit to the Minister a certificate stating the extent to which it is satisfied with the report and whether any of the Service's operational activities described in the report, in its opinion,

(a) is not authorized by or under this Act or contravenes any directions issued by the Minister under subsection 6(2); or

(b) involves an unreasonable or unnecessary exercise by the Service of any of its powers.

[...]

PRIVACY ACT, RSC, 1985, c P-21

Actions relating to international affairs and defence

51 (1) Any application under section 41 or 42 relating to personal information that the head of a government institution has refused to disclose by reason of paragraph 19(1)(a) or (b) or section

l'article 19 de la *Loi sur la citoyenneté*,

(iii) les affaires qui lui sont transmises en vertu de l'article 45 de la *Loi canadienne sur les droits de la personne*.

Examen des mesures

(1.1) Dans le cadre de la surveillance de la façon dont le Service exerce ses fonctions, le comité de surveillance examine à chaque exercice au moins un aspect de la prise, par le Service, de mesures pour réduire les menaces envers la sécurité du Canada.

Autres fonctions du comité de surveillance

(2) Dans les plus brefs délais possible après réception du rapport visé au paragraphe 6(4), le comité de surveillance remet au ministre un certificat indiquant dans quelle mesure le rapport lui paraît acceptable et signalant toute activité opérationnelle du Service visée dans le rapport qui, selon lui :

a) n'est pas autorisée sous le régime de la présente loi ou contrevient aux instructions données par le ministre en vertu du paragraphe 6(2);

b) comporte un exercice abusif ou inutile par le Service de ses pouvoirs.

[...]

LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS, LRC (1985), ch P-21

Affaires internationales et défense

51 (1) Les recours visés aux articles 41 ou 42 et portant sur les cas où le refus de donner communication de renseignements personnels est lié aux alinéas 19(1) a) ou b) ou à l'article 21 et

21, and any application under section 43 in respect of a file contained in a personal information bank designated as an exempt bank under section 18 to contain files all of which consist predominantly of personal information described in section 21, shall be heard and determined by the Chief Justice of the Federal Court or by any other judge of the Court that the Chief Justice may designate to hear the applications.

Special rules for hearings

(2) An application referred to in subsection (1) or an appeal brought in respect of such application shall

(a) be heard *in camera*; and

(b) on the request of the head of the government institution concerned, be heard and determined in the National Capital Region described in the schedule to the *National Capital Act*.

RADIOCOMMUNICATION ACT, RSC, 1985, c R-2

Minister's powers

5 (1) Subject to any regulations made under section 6, the Minister may, taking into account all matters that the Minister considers relevant for ensuring the orderly establishment or modification of radio stations and the orderly development and efficient operation of radiocommunication in Canada,

(a) issue

(i) radio licences in respect of radio apparatus,

sur les cas concernant la présence des dossiers dans chacun desquels dominant des renseignements visés à l'article 21 dans des fichiers inconsultables classés comme tels en vertu de l'article 18 sont exercés devant le juge en chef de la Cour fédérale ou tout autre juge de cette Cour qu'il charge de leur audition.

Règles spéciales

(2) Les recours visés au paragraphe (1) font, en premier ressort ou en appel, l'objet d'une audition à huis clos; celle-ci a lieu dans la région de la capitale nationale définie à l'annexe de la *Loi sur la capitale nationale* si le responsable de l'institution fédérale concernée le demande

LOI SUR LA RADIOCOMMUNICATION, LRC, ch R-2

Pouvoirs ministériels

5 (1) Sous réserve de tout règlement pris en application de l'article 6, le ministre peut, compte tenu des questions qu'il juge pertinentes afin d'assurer la constitution ou les modifications ordonnées de stations de radiocommunication ainsi que le développement ordonné et l'exploitation efficace de la radiocommunication au Canada :

a) délivrer et assortir de conditions :

(i) les licences radio à l'égard d'appareils radio, et notamment prévoir les conditions spécifiques relatives aux services pouvant être fournis par leur titulaire,

(i.1) spectrum licences in respect of the utilization of specified radio frequencies within a defined geographic area,

(ii) broadcasting certificates in respect of radio apparatus that form part of a broadcasting undertaking,

(iii) radio operator certificates,

(iv) technical acceptance certificates in respect of radio apparatus, interference-causing equipment and radio-sensitive equipment, and

(v) any other authorization relating to radiocommunication that the Minister considers appropriate,

and may fix the terms and conditions of any such licence, certificate or authorization including, in the case of a radio licence and a spectrum licence, terms and conditions as to the services that may be provided by the holder thereof

Prohibitions

9 (1) No person shall

(a) knowingly send, transmit or cause to be sent or transmitted any false or fraudulent distress signal, message, call or radiogram of any kind;

(b) without lawful excuse, interfere with or obstruct any radiocommunication;

(c) decode an encrypted subscription programming signal or encrypted network feed otherwise than under and in accordance with an authorization from the lawful distributor of the signal or feed;

(d) operate a radio apparatus so as to receive an encrypted subscription programming signal or

(i.1) les licences de spectre à l'égard de l'utilisation de fréquences de radiocommunication définies dans une zone géographique déterminée, et notamment prévoir les conditions spécifiques relatives aux services pouvant être fournis par leur titulaire,

(ii) les certificats de radiodiffusion à l'égard de tels appareils, dans la mesure où ceux-ci font partie d'une entreprise de radiodiffusion,

(iii) les certificats d'opérateur radio,

(iv) les certificats d'approbation technique à l'égard d'appareils radio, de matériel brouilleur ou de matériel radiosensible,

(v) toute autre autorisation relative à la radiocommunication qu'il estime indiquée;

Interdictions

9 (1) Il est interdit :

a) d'envoyer, d'émettre ou de faire envoyer ou émettre, sciemment, un signal de détresse ou un message, appel ou radiogramme de quelque nature, faux ou frauduleux;

b) sans excuse légitime, de gêner ou d'entraver la radiocommunication;

c) de décoder, sans l'autorisation de leur distributeur légitime ou en contravention avec celle-ci, un signal d'abonnement ou une alimentation réseau;

d) d'utiliser un appareil radio de façon à recevoir un signal d'abonnement ou une alimentation

encrypted network feed that has been decoded in contravention of paragraph (c); or

(e) retransmit to the public an encrypted subscription programming signal or encrypted network feed that has been decoded in contravention of paragraph (c).

CRIMINAL CODE, RSC, 1985, c C-46

Definitions

183 In this Part,

private communication

means any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it; (communication privée)

Interception

184 (1) Every one who, by means of any electromagnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.

Saving provision

(2) Subsection (1) does not apply to

réseau ainsi décodé;

e) de transmettre au public un signal d'abonnement ou une alimentation réseau ainsi décodé.

CODE CRIMINEL, LRC (1985), ch C-46

Définitions

183 Les définitions qui suivent s'appliquent à la présente partie.

communication privée

Communication orale ou télécommunication dont l'auteur se trouve au Canada, ou destinée par celui-ci à une personne qui s'y trouve, et qui est faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers. La présente définition vise également la communication radiotéléphonique traitée électroniquement ou autrement en vue d'empêcher sa réception en clair par une personne autre que celle à laquelle son auteur la destine. (private communication)

Interception

184 (1) Est coupable d'un acte criminel et passible d'un emprisonnement maximal de cinq ans quiconque, au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, intercepte volontairement une communication privée.

Réserve

(2) Le paragraphe (1) ne s'applique pas aux

personnes suivantes :

(a) a person who has the consent to intercept, express or implied, of the originator of the private communication or of the person intended by the originator thereof to receive it;

a) une personne qui a obtenu, de l'auteur de la communication privée ou de la personne à laquelle son auteur la destine, son consentement exprès ou tacite à l'interception;

(b) a person who intercepts a private communication in accordance with an authorization or pursuant to section 184.4 or any person who in good faith aids in any way another person who the aiding person believes on reasonable grounds is acting with an authorization or pursuant to section 184.4;

b) une personne qui intercepte une communication privée en conformité avec une autorisation ou en vertu de l'article 184.4, ou une personne qui, de bonne foi, aide de quelque façon une autre personne qu'elle croit, en se fondant sur des motifs raisonnables, agir en conformité avec une telle autorisation ou en vertu de cet article;

(c) a person engaged in providing a telephone, telegraph or other communication service to the public who intercepts a private communication,

c) une personne qui fournit au public un service de communications téléphoniques, télégraphiques ou autres et qui intercepte une communication privée dans l'un ou l'autre des cas suivants :

(i) if the interception is necessary for the purpose of providing the service,

(i) cette interception est nécessaire pour la fourniture de ce service,

(ii) in the course of service observing or random monitoring necessary for the purpose of mechanical or service quality control checks, or

(ii) à l'occasion de la surveillance du service ou d'un contrôle au hasard nécessaire pour les vérifications mécaniques ou la vérification de la qualité du service,

(iii) if the interception is necessary to protect the person's rights or property directly related to providing the service;

(iii) cette interception est nécessaire pour protéger ses droits ou biens directement liés à la fourniture d'un service de communications téléphoniques, télégraphiques ou autres;

(d) an officer or servant of Her Majesty in right of Canada who engages in radio frequency spectrum management, in respect of a private communication intercepted by that officer or servant for the purpose of identifying, isolating or preventing an unauthorized or interfering use of a frequency or of a transmission; or

d) un fonctionnaire ou un préposé de Sa Majesté du chef du Canada chargé de la régulation du spectre des fréquences de radiocommunication, pour une communication privée qu'il a interceptée en vue d'identifier, d'isoler ou d'empêcher l'utilisation non autorisée ou importune d'une fréquence ou d'une transmission;

(e) a person, or any person acting on their behalf, in possession or control of a computer system, as defined in subsection 342.1(2), who intercepts a private communication originating from, directed to or transmitting through that

e) une personne - ou toute personne agissant pour son compte - qui, étant en possession ou responsable d'un ordinateur - au sens du paragraphe 342.1(2) -, intercepte des communications privées qui sont destinées à celui-

computer system, if the interception is reasonably necessary for

(i) managing the quality of service of the computer system as it relates to performance factors such as the responsiveness and capacity of the system as well as the integrity and availability of the system and data, or

(ii) protecting the computer system against any act that would be an offence under subsection 342.1(1) or 430(1.1).

Use or retention

(3) A private communication intercepted by a person referred to in paragraph (2)(e) can be used or retained only if

(a) it is essential to identify, isolate or prevent harm to the computer system; or

(b) it is to be disclosed in circumstances referred to in subsection 193(2).

Colour of right

429 (2) No person shall be convicted of an offence under sections 430 to 446 where he proves that he acted with legal justification or excuse and with colour of right.

ci, en proviennent ou passent par lui, si l'interception est raisonnablement nécessaire :

(i) soit pour la gestion de la qualité du service de l'ordinateur en ce qui concerne les facteurs de qualité tels que la réactivité et la capacité de l'ordinateur ainsi que l'intégrité et la disponibilité de celui-ci et des données,

(ii) soit pour la protection de l'ordinateur contre tout acte qui constituerait une infraction aux paragraphes 342.1(1) ou 430(1.1).

Utilisation ou conservation

(3) La communication privée interceptée par la personne visée à l'alinéa (2) e) ne peut être utilisée ou conservée que si, selon le cas :

a) elle est essentielle pour détecter, isoler ou empêcher des activités dommageables pour l'ordinateur;

b) elle sera divulguée dans un cas visé au paragraphe 193(2).

Apparence de droit

429 (2) Nul ne peut être déclaré coupable d'une infraction visée aux articles 430 à 446 s'il prouve qu'il a agi avec une justification ou une excuse légale et avec apparence de droit.

FEDERAL COURT

SOLICITORS OF RECORD

DOCKETS:

██████████

STYLE OF CAUSE:

IN THE MATTER OF AN APPLICATION BY
██████████ PURSUANT TO SECTIONS 12 AND 21
OF THE *CANADIAN SECURITY INTELLIGENCE ACT*,
RSC 1985, c C-23 AND IN THE MATTER OF
ISLAMIST TERRORISM AND ██████████

PLACE OF HEARING:

OTTAWA, ONTARIO

DATE OF HEARING:

MARCH 17, 2017 AND MAY 4, 2017

**PUBLIC JUDGMENT AND
REASONS:**

CRAMPTON C.J.

DATED:

SEPTEMBER 27, 2017

APPEARANCES:

Ms. Jennifer Poirier
Ms. Stéphanie Dion
Ms. Ilana Bleichert

DEPARTMENT OF JUSTICE
NATIONAL SECURITY LITIGATION
AND ADVISORY GROUP

Mr. Gordon Cameron
Mr. Owen Rees

AMICUS CURIAE

SOLICITORS OF RECORD:

Attorney General of Canada
Ottawa, Ontario

DEPARTMENT OF JUSTICE
NATIONAL SECURITY LITIGATION
AND ADVISORY GROUP

Blakes Cassels & Graydon LLP
Ottawa, Ontario

BARRISTERS AND SOLICITORS

Conway Baxter Wilson LLP
Ottawa, Ontario