TOP SECRET
CONF-2-17
2017 FC 1047

IN THE MATTER of an Application by [***] for Warrants Pursuant to Sections 12 and 21 of the *Canadian Security Intelligence Service Act*, R.S.C., 1985, c. C-23

and

IN THE MATTER of Islamist Terrorism and [***]

Indexed as: X (Re)

Federal Court, Crampton C.J.—Ottawa, March 17, May 4 and September 27, 2017.

Editor's Note: Portions redacted by the Court are indicated by [***].

Security Intelligence — Reference seeking to determine whether information obtained by Canadian Security Intelligence Service (CSIS) from mobile devices of subject of investigation (subject) unlawful — CSIS capturing International Mobile Subscriber Identity (IMSI), International Mobile Equipment Identity (IMEI) numbers with cellular-site simulator (CSS) — CSIS using CSS technology to attribute cellular device to subject whose identity already known, to "geo-locate" subject's cellular device — Attorney General submitting, inter alia, use of CSS not contravening Radiocommunication Act, s. 9(1)(b), Criminal Code, s. 184, Canadian Charter of Rights and Freedoms, s. 8 — Whether CSIS's use of CSS without warrant to obtain identifying characteristics of subject's mobile devices unlawful — CSIS's use of CSS technology not contravening Radiocommunication Act — Wording of Authority to Use Radio held by CSIS in accordance with Radiocommunication Act, s. 5(1)(a)(v) sufficiently broad to cover use of CSS equipment by CSIS — CSIS also not contravening Criminal Code — Obtaining IMSI, IMEI identifiers through use of CSS equipment not capturing any content of communications made by targeted mobile devices — – Criminal Code mischief provisions also not violated — As to Charter, s. 8, while capture of IMSI, IMEI constituting "search", such capture only minimally intrusive and is authorized by law — Nothing in language of Canadian Security Intelligence Service Act (Act), s. 21, or elsewhere supporting view that CSIS required to obtain warrant when engaging in minimally intrusive "search" — Act, s. 12 providing CSIS with authority to investigate suspicious

TRÈS SECRET
CONF-2-17
2017 CF 1047

DANS L'AFFAIRE d'une demande de mandat présentée par [***] en vertu des articles 12 et 21 de la *Loi sur le service canadien du renseignement de sécurité*, L.R.C. (1985), ch. C-23

et

DANS L'AFFAIRE VISANT le terrorisme islamiste et [***]

Répertorié : X (Re)

Cour fédérale, juge en chef Crampton—Ottawa, 17 mars, 4 mai et 27 septembre 2017.

Note de l'arrêtiste : Les parties caviardées par la Cour sont indiquées par [***].

Renseignement de sécurité — Renvoi visant à déterminer si l'information obtenue par le Service canadien du renseignement de sécurité (SCRS) des appareils mobiles de la cible connue d'une enquête (cible) était illégale — Le SCRS a utilisé un émulateur de station de base (ESB) pour obtenir les numéros de l'identité internationale de l'abonné mobile (IMSI) et de l'identité internationale d'équipement mobile (IMEI) — Le SCRS a utilisé la technologie relative aux ESB pour attribuer un appareil cellulaire à une cible dont l'identité est déjà connue et pour géolocaliser l'appareil cellulaire de la cible — La procureure générale a soutenu notamment que l'utilisation de la technologie relative aux ESB n'avait enfreint ni l'art. 9(1)b) de la Loi sur la radiocommunication, ni l'art. 184 du Code criminel, ni l'art. 8 de la Charte canadienne des droits et libertés — Il s'agissait de déterminer si l'utilisation par le SCRS d'un ESB sans mandat dans le but d'obtenir les caractéristiques distinctives des appareils mobiles de la cible était illégale — L'utilisation par le SCRS de la technologie relative aux ESB n'a pas contrevenu à la Loi sur la radiocommunication — Le libellé de l'Autorisation relative à l'utilisation d'appareils radio que détenait le SCRS conformément à l'art. 5(1)(a)(v) de la Loi sur la radiocommunication était assez général pour inclure l'utilisation d'ESB et du matériel connexe par le SCRS — Le SCRS n'a pas contrevenu non plus au Code criminel — L'obtention des identificateurs de l'IMSI et de l'IMEI au moyen d'un ESB n'équivaut pas à la capture de tout contenu de communications effectuée au moyen des appareils mobiles visés — – Le SCRS n'a pas enfreint non plus les dispositions du Code criminel

activities without warrant — View that CSIS requiring warrant every time that person's reasonable expectation of privacy engaged reading out requirement that search be "unreasonable" before it may be found contrary to Charter, s. 8 — Parliament implicitly allowing CSIS to use CSS when passing s. 12 — S. 12 reasonable law — "Reasonable grounds to suspect" standard sufficient to justify warrantless search — National security objectives sufficient to tip balance in favour of state interest when searches minimally intrusive — S. 12 neither overbroad nor vague — Scope of information CSIS may collect, retain limited to that which is "strictly necessary" — S. 12 not lacking in precision — Clearly articulating scope of activities to be investigated by CSIS — Judicial pre-authorization under Act, s. 21 necessary for more than minimally intrusive activities — Judgment: CSIS's warrantless use of CSS technology to capture identifying characteristics of subject's mobile devices not unlawful

Constitutional Law — Charter of Rights — Unreasonable Search or Seizure — Canadian Security Intelligence Service (CSIS) capturing, without warrant, International Mobile Subscriber Identity (IMSI), International Mobile Equipment Identity (IMEI) numbers from mobile devices of subject of investigation (subject) with cellular-site simulator (CSS) — Attorney General submitting, inter alia, use of CSS not contravening Charter, s. 8 — Whether subject's Charter, s. 8 rights violated — Specifically, whether CSIS conducting "search or seizure", whether search or seizure "reasonable" — Individuals having reasonable expectation of privacy in respect of IMSI, IMEI identifiers — Capture of IMSI, IMEI identifiers therefore constituting "search" — However, such capture only minimally intrusive — CSIS not requiring warrant whenever wishing to gather information through use of new technology — Supreme Court making it clear there is no free-standing prohibition on use of electronic or other technologies without a warrant — Rather, question whether technology intruding on reasonable sphere of privacy of individual — Here, nothing about CSS technology per se justifying conclusion that its use objectively unreasonable — Minimally invasive search not

sur les méfaits — En ce qui concerne l'art. 8 de la Charte, la collecte de l'IMSI et de l'IMEI constituait une « fouille », mais cette collecte n'était que minimalement envahissante et elle était autorisée par la loi — Ni le libellé de l'art. 21 ni les autres dispositions de la Loi sur le Service canadien du renseignement de sécurité (Loi sur le SCRS) n'appuient le point de vue selon lequel le SCRS doit obtenir un mandat chaque fois qu'il effectue une « fouille » minimalement envahissante — Le libellé de l'art. 12 de la Loi sur le SCRS confère au SCRS le pouvoir d'enquêter sans mandat sur des activités suspectes — Considérer que le SCRS doit obtenir un mandat chaque fois que les attentes raisonnables d'une personne en matière de vie privée sont en jeu rendrait inopérante l'exigence voulant qu'une fouille doit être « abusive » pour enfreindre l'art. 8 de la Charte — Le Parlement a implicitement permis au SCRS d'utiliser un ESB lorsqu'il a adopté l'art. 12 — L'art. 12 est une disposition législative raisonnable — Le critère des « motifs raisonnables de soupçonner » suffit à justifier une fouille sans mandat — Les objectifs relatifs à la sécurité nationale suffisent à faire pencher la balance en faveur des intérêts de l'État lorsque les fouilles sont minimalement envahissantes — L'art. 12 ni n'a une portée excessive, ni n'est vague — La portée des informations qui peuvent être recueillies par le SCRS est limitée à ce qui « est strictement nécessaire » — L'art. 12 ne manque pas de précision — Il formule clairement la portée des activités qui peuvent faire l'objet d'une enquête par le SCRS — L'autorisation judiciaire préalable au titre de l'art. 21 de la Loi sur le SCRS est nécessaire pour les activités de collecte plus que minimalement envahissantes — Jugement : l'utilisation sans mandat par le SCRS de la technologie relative aux ESB pour capturer les caractéristiques distinctives des appareils mobiles de la cible n'était pas illégale.

Droit constitutionnel — Charte des droits — Fouilles, perquisitions ou saisies abusives — Le Service canadien du renseignement de sécurité (SCRS) a utilisé un émulateur de station de base (ESB) pour obtenir sans mandat les numéros de l'identité internationale de l'abonné mobile (IMSI) et de l'identité internationale d'équipement mobile (IMEI) des appareils mobiles de la cible d'une enquête (cible) — La procureure générale a soutenu notamment que l'utilisation d'un ESB n'avait pas enfreint l'art. 8 de la Charte — Il s'agissait de déterminer s'il a été contrevenu aux droits garantis par l'art. 8 de la Charte — Plus particulièrement, il s'agissait de déterminer si le SCRS a effectué une « fouille, une perquisition ou une saisie » et, le cas échéant, si elle était « raisonnable » — Les particuliers ont une attente raisonnable en matière de vie privée à l'endroit des indicateurs de l'IMSI et de l'IMEI — La collecte des identificateurs de l'IMSI et de l'IMEI constitue donc une « fouille » — Toutefois, cette collecte n'est que minimalement envahissante — Le SCRS ne doit pas toujours obtenir un mandat lorsqu'il désire recueillir des informations au moyen d'une nouvelle technologie — La Cour suprême a clairement indiqué qu'il n'y a pas d'interdiction distincte visant l'utilisation sans

necessarily contravening s. 8 — CSS technology reliable, not giving rise to consequences associated with "false positive" — CSIS's CSS operations not unreasonable.

Radiocommunications — Canadian Security Intelligence Service (CSIS) capturing International Mobile Subscriber Identity (IMSI), International Mobile Equipment Identity (IMEI) numbers from mobile devices of subject of investigation with cellular-site simulator (CSS) — CSIS holding Authority to Use Radio (Authority) in accordance with Radiocommunication Act, s. 5(1)(a)(v) — Wording of Authority sufficiently broad to cover use of CSS equipment by CSIS.

Criminal Justice — Canadian Security Intelligence Service (CSIS) capturing, without warrant, International Mobile Subscriber Identity (IMSI), International Mobile Equipment Identity (IMEI) numbers from subject of investigation with cellular-site simulator (CSS) — CSIS use of CSS without judicial authorization not contravening Criminal Code, s. 184 as no content of communications made by targeted mobile devices captured — Criminal Code mischief provisions also not violated.

This was a reference seeking to determine whether the activity in which the Canadian Security Intelligence Service (CSIS) engaged to obtain information from the mobile devices of a known subject of investigation (subject) was unlawful.

The activity in question was conducted without a warrant and involved CSIS's use of a cellular-site simulator (CSS) to capture the identifying characteristics of the mobile devices, which consisted of the International Mobile Subscriber Identity (IMSI) and International Mobile Equipment Identity (IMEI) numbers that were emitted by the mobile devices when they attempted to communicate with the cellular network of the telecommunications service providers (TSP). The IMSI number identified the country in which the subject's cellular account is located, the network code of his TSP, and the unique subscriber identifying number given to the subject by the TSP. The IMEI identified the make, model and unique serial number of his mobile devices. CSIS currently only uses CSS technology for two purposes: (1) to attribute a cellular device to a subject

mandat de techniques, électroniques ou autres — La question à poser était plutôt celle de savoir si la technologie constituait une intrusion dans la sphère raisonnable de vie privée des particuliers — En l'espèce, il n'y avait rien qui soit relié à l'utilisation de la technologie relative aux ESB en soi qui permette de conclure que cette utilisation était objectivement déraisonnable — La fouille minimalement envahissante ne contrevient pas nécessairement à l'art. 8 — La technologie relative aux ESB est fiable et elle ne peut pas entraîner de conséquences ayant trait à un «faux positif» — L'utilisation par le SCRS de la technologie relative aux ESB n'était pas déraisonnable.

Radiocommunications — Le Service canadien du renseignement de sécurité (SCRS) a utilisé un émulateur de station de base (ESB) pour obtenir les numéros de l'identité internationale de l'abonné mobile (IMSI) et de l'identité internationale d'équipement mobile (IMEI) des appareils mobiles de la cible d'une enquête — Le SCRS détenait une Autorisation relative à l'utilisation d'appareils radio (Autorisation) conformément à l'art. 5(1)(a)(v) de la Loi sur la radiocommunication — Le libellé de l'Autorisation était assez général pour inclure l'utilisation d'un ESB et du matériel connexe par le SCRS.

Justice criminelle et pénale — Le Service canadien du renseignement de sécurité (SCRS) a utilisé un émulateur de station de base (ESB) pour obtenir sans mandat les numéros de l'identité internationale de l'abonné mobile (IMSI) et de l'identité internationale d'équipement mobile (IMEI) de la cible d'une enquête — L'utilisation d'ESB par le SCRS sans une autorisation judiciaire n'a pas contrevenu à l'art. 184 du Code criminel, car elle n'a permis de capturer aucun contenu de communications effectuées au moyen des appareils mobiles visés — Cela n'a pas enfreint non plus les dispositions du Code criminel sur les méfaits.

Il s'agissait d'un renvoi visant à déterminer si l'activité menée par le Service canadien du renseignement de sécurité (SCRS) pour tirer de l'information des appareils mobiles de la cible connue d'une enquête (cible) était illégale.

L'activité en question a été menée sans mandat et comprenait l'utilisation d'un émulateur de station de base (ESB) pour obtenir les caractéristiques distinctives des appareils mobiles, qui consistaient en l'identité internationale de l'abonné mobile (IMSI) et en l'identité internationale d'équipement mobile (IMEI), des numéros émis par les appareils mobiles lorsqu'ils ont tenté de communiquer avec le réseau cellulaire des fournisseurs de services de télécommunication (FST). L'IMSI indiquait le pays où se trouvait le compte de téléphonie cellulaire auquel était abonnée la cible, le code de réseau de son FST et le numéro d'identification unique que lui avait attribuée le FST. L'IMEI précisait la marque, le modèle et le numéro de série de ses appareils mobiles. Le SCRS n'utilise actuellement la technologie relative aux ESB qu'à deux fins : 1) attribuer un

of investigation whose identity is already known, and (2) to "geo-locate" a subject of investigation's cellular device.

The Attorney General submitted, *inter alia*, that CSIS's use of CSS technology solely to capture IMSI and IMEI identifiers does not contravene the *Radiocommunication Act*, the *Criminal Code* or the *Canadian Charter of Rights and Freedoms* (Charter). Specifically, the Attorney General maintained that CSIS's use of a CSS complies with the *Radiocommunication Act* because CSIS holds an Authority to Use Radio (Authority) in accordance with subparagraph 5(1)(a)(v) of the *Radiocommunication Act* and that, by virtue of that Authority and section 12 of the *Canadian Security Intelligence Service Act* (the Act), CSIS's use of CSS technology does not contravene paragraph 9(1)(b) of the *Radiocommunication Act.* CSIS also maintained 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.

The main issue was whether CSIS's use of a CSS without a warrant, and solely to obtain the identifying characteristics of the subject's mobile devices, was unlawful.

Held, CSIS's warrantless use of CSS technology to capture the identifying characteristics of the subject's mobile devices was not unlawful.

CSIS's use of CSS technology does not contravene the *Radiocommunication Act*. On its face, the wording of the Authority is sufficiently broad to cover the use of CSS equipment by CSIS. 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. 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. Those words have the effect of allowing the Authority to be used in respect of such radio apparatus.

Obtaining IMSI and IMEI identifiers through the use of CSS equipment does not capture any content of communications made by the mobile devices that are targeted by that equipment. Accordingly, 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*. CSIS's use of a CSS without a warrant also does not contravene the mischief

appareil cellulaire à une cible dont l'identité est déjà connue, et 2) géolocaliser l'appareil cellulaire de la cible.

La procureure générale a soutenu notamment que l'utilisation de la technologie relative aux ESB par le SCRS à la seule fin de recueillir des indicateurs de l'IMSI et de l'IMEI n'enfreint ni la *Loi sur la radiocommunication*, ni le *Code criminel*, ni la *Charte canadienne des droits et libertés* (la Charte). Ella a fait valoir plus particulièrement que l'utilisation par le SCRS de la technologie relative aux ESB est conforme à la *Loi sur la radiocommunication* parce que le SCRS détient une autorisation relative à l'utilisation d'appareils radio (Autorisation) en vertu du sous-alinéa 5(1)a)(v) de la *Loi sur la radiocommunication* et qu'au titre de l'Autorisation et de l'article 12 de la *Loi sur le Service canadien du renseignement de sécurité* (la Loi sur le SCRS), l'utilisation que fait le SCRS de la technologie relative aux ESB ne contrevient pas à l'alinéa 9(1)b) de la *Loi sur la radiocommunication.* Le SCRS a soutenu également qu'il n'avait pas contrevenu à l'article 184 du *Code criminel* en utilisant des ESB sans avoir obtenu d'autorisation judiciaire au préalable parce que les appareils en question n'interceptent aucune communication privée.

Il s'agissait principalement de déterminer si l'utilisation par le SCRS d'un ESB sans mandat dans le seul but d'obtenir les caractéristiques distinctives des appareils mobiles de la cible était illégale.

Jugement : l'utilisation sans mandat par le SCRS de la technologie relative aux ESB pour capturer les caractéristiques distinctives des appareils mobiles de la cible n'était pas illégale.

L'utilisation que fait le SCRS de la technologie relative aux ESB ne contrevient pas à la *Loi sur la radiocommunication*. À première vue, le libellé de l'Autorisation est assez général pour inclure l'utilisation d'ESB et du matériel connexe par le SCRS. En particulier, la portée du segment « relativement à tous les types d'appareils radio spécialement conçus aux fins indiquées au paragraphe 2 », qui figure au paragraphe 1 de l'Autorisation, englobe clairement l'utilisation de ce genre de matériel. Ce segment semble indiquer qu'il a été envisagé, lorsque l'Autorisation a été délivrée, qu'elle allait être invoquée à l'endroit d'appareils radio qui n'existaient pas en 1992. En raison de ce segment, l'Autorisation peut être invoquée à l'endroit de tels appareils radio.

L'obtention d'indicateurs de l'IMSI et de l'IMEI au moyen d'ESB ne peut être assimilée à la capture de tout contenu de communications effectuée au moyen des appareils mobiles visés. Par conséquent, l'utilisation que fait le SCRS de la technologie relative aux ESB en vue d'attribuer des IMSI et des IMEI à une cible ne contrevient pas à la Partie VI du *Code criminel*. L'utilisation d'un ESB sans mandat par le SCRS

provisions in section 430 of the *Criminal Code*. Section 12 of the Act and the Authority provide a lawful exemption from conviction under section 429 of the *Criminal Code*.

There were two distinct issues to be assessed in determining whether there was a violation of section 8 of the Charter, namely (i) whether there was a "search or seizure", and (ii), if so, whether that search or seizure was "unreasonable". A consideration of the totality of the circumstances, and taking a purposive approach to section 8 of the Charter, suggests that individuals have a reasonable expectation of privacy in respect of the IMSI and IMEI identifiers. This is because of the nature of the information that those numbers permit CSIS to obtain or infer. The use of CSS technology therefore constitutes a "search". 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. In addition, 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 devices. There is no 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.

CSS technology is minimally intrusive. Neither the mobile device nor its contents are accessed in any way. Although CSIS may be able to begin putting together an initial profile of the subject of investigation 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.

CSIS does not require a warrant whenever it wishes to gather information through the use of new technology. The Supreme Court made it clear that there is no "free-standing prohibition on [the use of] electronic or other technologies without a warrant." Rather, the question is whether the technology intrudes 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 this particular case, there was nothing about CSS technology *per se* that would justify a conclusion that its use is objectively unreasonable. Individuals' subjective expectations of privacy in relation to the IMSI and IMEI information on their mobile devices are objectively reasonable.

n'enfreint pas non plus les dispositions de l'article 430 du *Code criminel* sur les méfaits. L'article 12 de la Loi sur le SCRS et l'Autorisation fournissent des exemptions légitimes à une déclaration de culpabilité fondée sur l'article 429 du *Code criminel*.

Deux questions distinctes ont dû être étudiées pour déterminer s'il y avait eu infraction à l'article 8 de la Charte : i) la possibilité qu'il y ait eu une « fouille, une perquisition ou une saisie » et, dans l'affirmative ii), la possibilité qu'elle ait été abusive. La prise en considération de l'ensemble des circonstances et l'adoption d'une approche téléologique à l'égard de l'article 8 de la Charte donnent à penser que les particuliers ont une attente raisonnable en matière de vie privée à l'endroit des indicateurs de l'IMSI et de l'IMEI. C'est en raison de la nature de l'information que ces numéros permettent au SCRS d'obtenir ou d'inférer. Partant, l'utilisation de la technologie relative aux ESB constitue une « fouille ». Il est possible de présumer qu'en général, les personnes ont vraisemblablement l'attente subjective que toute information relative à leurs appareils mobiles susceptible d'être communiquée aux tours de téléphonie cellulaire relevant de leur FST ne sera pas interceptée subrepticement par des agents de l'État, comme le SCRS. De plus, la moyenne des gens ne croit vraisemblablement pas avoir « abandonné » l'IMSI et l'IMEI lorsque l'appareil mobile communique ces identificateurs aux tours de téléphonie cellulaire. Il n'y a pas de renonciation implicite aux droits en matière de vie privée à l'endroit du grand public en ce qui a trait à l'IMSI et à l'IMEI lorsque les appareils mobiles communiquent ces informations dans un environnement cellulaire.

La technologie relative aux ESB est minimalement envahissante. Ni l'appareil mobile ni son contenu n'est consulté d'aucune façon. Alors que le SCRS peut commencer à dresser un profil initial de la cible et de ses habitudes de communication, il est difficile de voir comment il pourrait en tirer des conclusions qui seraient particulièrement justes ou auraient un caractère envahissant concernant les activités personnelles de cette personne.

Le SCRS ne doit pas toujours obtenir un mandat lorsqu'il désire recueillir des informations au moyen d'une nouvelle technologie. La Cour suprême du Canada a clairement indiqué qu'il n'y a pas « d'interdiction distincte visant l'utilisation sans mandat de techniques, électroniques ou autres. » La question à poser est plutôt celle de savoir si la technologie constitue une intrusion dans la sphère raisonnable de vie privée des personnes surveillées. La réponse à cette question nécessite une évaluation de l'ensemble des circonstances pertinentes. En l'espèce, il n'y avait rien qui soit relié à l'utilisation de la technologie relative aux ESB en soi qui permette de conclure que cette utilisation est objectivement déraisonnable. Les attentes subjectives d'une personne en matière de vie privée quant aux IMSI et aux IMEI liées à ses appareils mobiles sont objectivement raisonnables.

In conclusion, regarding whether the capture of IMSI and IMEI identifiers constitutes a "search", although intrusions on individuals' anonymity interests do not always engage section 8 of the Charter, 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. 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.

CSIS's use of a CSS to intercept and attribute the IMSI and IMEI numbers of a mobile device is authorized by law. 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 of the Act 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 one is required at common law. 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. Parliament implicitly allowed 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", when it passed section 12 of the Act.

The nature and purpose of section 12 support the view that it is a reasonable law. The "reasonable grounds to suspect" standard set forth in section 12 of the Act is sufficient to justify a warrantless search by CSIS. 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. Section 12 is neither overbroad nor vague, because it imposes objective standards and strict limits on the collection of information by CSIS. The scope of information that may be collected by CSIS is explicitly limited to that which "is strictly necessary". This limitation also implicitly applies to the retention of information collected by CSIS. 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". On the contrary, section 12, read together with the definition of "threats to the

En conclusion, en ce qui concerne la question de savoir si la collecte des identificateurs de l'IMSI et de l'IMEI constitue une « fouille », alors que les atteintes au droit à l'anonymat d'une personne n'ont pas toujours trait à l'article 8 de la Charte, c'est le cas de la collecte de l'IMSI et de l'IMEI en raison des profils que le SCRS peut commencer à esquisser en se fondant sur ces informations. Ce sont ces profils mêmes qui peuvent, en fin de compte, aider le SCRS à obtenir un mandat pour obtenir des informations sur l'abonné et entreprendre des activités encore plus envahissantes. Toutefois, jusqu'à ce que le SCRS soit en mesure d'obtenir des informations sur l'abonné et d'exercer d'autres pouvoirs conférés par un mandat, la collecte de l'IMSI et de l'IMEI n'est que minimalement envahissante.

L'utilisation, par le SCRS, d'un ESB pour intercepter l'IMSI et l'IMEI d'un appareil mobile pour attribuer celui-ci à une cible est autorisée par la loi. Ni le libellé de l'article 21 ni les autres dispositions de la Loi sur le SCRS n'appuient le point de vue selon lequel le SCRS doit obtenir un mandat chaque fois qu'il effectue une fouille ou une perquisition, au sens de la Charte, qui est minimalement envahissante. Le libellé de l'article 12 de la Loi sur le SCRS confère au SCRS toute la latitude nécessaire pour enquêter sans mandat sur des activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada, sauf si la common law l'exige. Considérer que le SCRS doit obtenir un mandat chaque fois que les attentes raisonnables d'une personne en matière de vie privée sont en jeu confondrait les deux éléments de l'article 8 de la Charte en un seul, c'est-à-dire que cela rendrait inopérante l'exigence voulant qu'une fouille doit être « abusive » pour enfreindre l'article 8. Le Parlement a implicitement permis au SCRS d'utiliser un ESB pour intercepter l'IMSI et l'IMEI d'un appareil mobile pour attribuer celui-ci à une cible selon des « motifs raisonnables de soupçonner » lorsqu'il a adopté l'article 12 de la Loi sur le SCRS.

La nature et l'objet de l'article 12 soutiennent l'opinion selon laquelle il s'agit d'une disposition législative raisonnable. Le critère des « motifs raisonnables de soupçonner » prévu à l'article 12 de la Loi sur le SCRS suffit à justifier que le SCRS effectue une fouille sans mandat. Les objectifs relatifs à la sécurité nationale qui figurent à l'article 12 suffiront habituellement à faire pencher la balance en faveur des intérêts de l'État, lorsque les fouilles menées par le SCRS sont minimalement envahissantes. L'article 12 ni n'a une portée excessive, ni n'est vague, car il impose des critères objectifs et des limites strictes à la collecte d'informations par le SCRS. La portée des informations qui peuvent être recueillies par le SCRS est explicitement limitée à ce qui « est strictement nécessaire ». Cette limite s'applique également de façon implicite à la conservation des informations recueillies par le SCRS. Compte tenu de ces limites facilement vérifiables et compréhensibles, on ne saurait affirmer que l'article 12

security of Canada" set forth in section 2 of the Act, clearly articulates the scope of activities that may be investigated by CSIS. 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.

The case law 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. The Supreme Court of Canada trilogy of "sniffer dog" cases, i.e. *R. v. A.M.*, *R. v. Kang-Brown* and *R. v. Chehil* 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 CSS technology is highly reliable and therefore does not give rise to the potentially severe consequences associated with a "false positive". The roles and responsibilities of the Minister, the Security Intelligence Review Committee and CSIS's Director 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. The manner in which CSIS currently conducts its CSS operations is not unreasonable.

« manque de précision au point de ne pas constituer un guide suffisant pour un débat judiciaire ». Au contraire, l'article 12, examiné en corrélation avec la définition de « menaces envers la sécurité du Canada » figurant à l'article 2 de la Loi sur le SCRS, formule clairement la portée des activités qui peuvent faire l'objet d'une enquête par le SCRS. En ajoutant les dispositions de l'article 21 concernant les mandats à la Loi sur le SCRS, le législateur prévoyait implicitement que le SCRS ne mènerait pas, en vertu de l'article 12, d'activités de collecte plus que minimalement envahissantes sans obtenir une autorisation judiciaire préalable au titre de l'article 21.

La jurisprudence sur laquelle s'appuient les *amici* n'étaye pas la proposition selon laquelle une fouille minimalement envahissante contrevient nécessairement à l'article 8 de la Charte en l'absence d'une autorisation judiciaire préalable ou d'un contrôle judiciaire a posteriori. La trilogie des affaires de « chiens renifleurs » de la Cour suprême du Canada (*Kang-Brown*, *A.M.* et *Chehil*) se distinguent de celles qui concernent l'utilisation, par le SCRS, de la technologie relative aux ESB pour recueillir l'IMSI et l'IMEI des appareils électroniques sans fil d'une personne, car cette technologie est très fiable et ne peut donc pas entraîner d'éventuelles conséquences graves ayant trait à un « faux positif ». Les rôles et les responsabilités du ministre, du Comité de surveillance des activités de renseignement de sécurité et du directeur du SCRS permettent de s'assurer que l'article 12 est une disposition législative raisonnable lorsqu'il s'agit d'évaluer le caractère minimalement envahissant des fouilles qu'il autorise. La façon dont le SCRS mène ses opérations fondées sur des ESB n'est pas abusive.

STATUTES AND REGULATIONS CITED

Canadian Charter of Rights and Freedoms, being Part I of the *Constitution Act, 1982*, Schedule B, *Canada Act 1982*, 1982, c. 11 (U.K.) [R.S.C., 1985, Appendix II, No. 44], s. 8.
Canadian Security Intelligence Service Act, R.S.C., 1985, c. C-23, ss. 2 "threats to the security of Canada", 6, 12, 16, 20(2),(3),(4), 21, 21.1(1),(3),(4), 22, 27, 34(1), 38(1).
Code of Conduct Regulation, Alta. Reg. 160/2003, s. 10(3)(f).
Criminal Code, R.S.C., 1985, c. C-46, ss. 183 " intercept", private communication", 184, 429, 430, 487.01, 492.2.
Electric Utilities Act, S.A. 2003, c. E-5.1.
Privacy Act, R.S.C., 1985, c. P-21, s. 51(2)(a).
Radiocommunication Act, R.S.C., 1985, c. R-2, ss. 2 "harmful interference", 5(1)(a), 9(1)(b).

LOIS ET RÈGLEMENTS CITÉS

Charte canadienne des droits et libertés, qui constitue la partie I de la *Loi constitutionnelle de 1982*, annexe B, *Loi de 1982 sur le Canada*, 1982, ch. 11 (R.-U.) [L.R.C. (1985), appendice II, no 44], art. 8.
Code criminel, L.R.C. (1985), ch. C-46, art. 183 « communication privée », « intercepter », 184, 429, 430, 487.01, 492.2.
Code of Conduct Regulation , Alta. Reg. 160/2003, s. 10(3)(f).
Electric Utilities Act, S.A. 2003, c. E-5.1.
Loi sur la protection des renseignements personnels, L.R.C. (1985), ch. P-21, art. 51(2)a).
Loi sur la radiocommunication, L.R.C. (1985), ch. R-2, art. 2 « brouillage préjudiciable », 5(1)a), 9(1)b).
Loi sur le Service canadien du renseignement de sécurité, L.R.C. (1985), ch. C-23, art. 2 « menaces envers la sécurité du Canada », 6, 12, 16, 20(2),(3),(4), 21, 21.1(1),(3),(4), 22, 27, 34(1), 38(1).

CASES CITED

FOLLOWED:

X (Re), 2016 FC 1105, [2017] 2 F.C.R. 396.

APPLIED:

R. v. Gomboc, 2010 SCC 55, [2010] 3 S.C.R. 211; *R. v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212; *Thomson Newspapers Ltd. v. Canada (Director of Investigation and Research, Restrictive Trade Practices Commission)*, [1990] 1 S.C.R. 425, (1990), 67 D.L.R. (4th) 161; *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432 (also distinguished on another ground); *R. v. Plant*, [1993] 3 S.C.R. 281, (1993), 145 A.R. 104 (also distinguished on another ground); *R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579; *Hunter et al. v. Southam Inc*, [1984] 2 S.C.R. 145, (1984), 55 A.R. 291; *R. v. Chehil*, 2013 SCC 49, [2013] 3 S.C.R. 220 (also distinguished on another ground); *R. v. Kang-Brown*, 2008 SCC 18, [2008] 1 S.C.R. 456 (also distinguished on another ground.

DISTINGUISHED:

R. v. A.M., 2008 SCC 19, [2008] 1 S.C.R. 569 (also considered on another ground); *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432 (also applied on another ground); *R. v. Plant*, [1993] 3 S.C.R. 281, (1993), 145 A.R. 104 (also applied on another ground); *Goodwin v. British Columbia (Superintendent of Motor Vehicles)*, 2015 SCC 46, [2015] 3 S.C.R. 250 (also considered on another ground); *R. v. Chehil*, 2013 SCC 49, [2013] 3 S.C.R. 220 (also applied on another ground); *R. v. Kang-Brown*, 2008 SCC 18, [2008] 1 S.C.R. 456 (also applied on another ground).

CONSIDERED:

Canadian Security Intelligence Service Act (Re), 2008 FC 300, [2008] 3 F.C.R. 477; *Canada (Citizenship and Immigration) v. Harkat*, 2014 SCC 37, [2014] 2 S.C.R. 33; *Ruby v. Canada (Solicitor General)*, 2002 SCC 75, [2002] 4 S.C.R. 3; *R. v. Brewster*, 2016 ONSC 4133 (CanLII); *R. v. A.M.*, 2008 SCC 19, [2008] 1 S.C.R. 569 (also distinguished on another ground); *R. v. Jarvis*, 2002 SCC 73, [2002] 3 S.C.R. 757; *R. v. Rodgers*, 2006 SCC 15, [2006] 1 S.C.R. 554; *Goodwin v. British Columbia (Superintendent of Motor Vehicles)*, 2015 SCC 46, [2015] 3 S.C.R. 250 (also distinguished on another ground); *Mahjoub (Re)*, 2013 FC 1096, 457 F.T.R. 1; *Canada Trustco Mortgage Co. v. Canada*, 2005 SCC 54, [2005] 2 S.C.R. 602; *Mahjoub v. Canada (Citizenship and Immigration)*, 2017 FCA 157, 387 C.R.R. (2d) 1; *Charkaoui v. Canada (Citizenship and Immigration)*,

JURISPRUDENCE CITÉE

DÉCISION SUIVIE :

X (Re), 2016 CF 1105, [2017] 2 R.C.F. 396.

DÉCISIONS APPLIQUÉES :

R. c. Gomboc, 2010 CSC 55, [2010] 3 R.C.S. 211; *R. c. Spencer*, 2014 CSC 43, [2014] 2 R.C.S. 212; *Thomson Newspapers Ltd. c. Canada (Directeur des enquêtes et recherches, Commission sur les pratiques restrictives du commerce)*, [1990] 1 R.C.S. 425; *R. c. Tessling*, 2004 CSC 67, [2004] 3 R.C.S. 432 (aussi différenciée pour un autre motif); *R. c. Plant*, [1993] 3 R.C.S. 281 (aussi différenciée pour un autre motif); *R. c. Patrick*, 2009 CSC 17, [2009] 1 R.C.S. 579; *Hunter et autres c. Southam Inc*, [1984] 2 R.C.S. 145; *R. c. Chehil*, 2013 CSC 49, [2013] 3 R.C.S. 220 (aussi différenciée pour un autre motif); *R. c. Kang-Brown*, 2008 CSC 18, [2008] 1 R.C.S. 456 (aussi différenciée pour un autre motif).

DÉCISIONS DIFFÉRENCIÉES :

R. c. A.M., 2008 CSC 19, [2008] 1 R.C.S. 569 (aussi examinée pour un autre motif); *R. c. Tessling*, 2004 CSC 67, [2004] 3 R.C.S. 432 (aussi appliquée pour un autre motif); *R. c. Plant*, [1993] 3 R.C.S. 281 (aussi appliquée pour un autre motif); *Goodwin c. Colombie-Britannique (Superintendent of Motor Vehicles)*, 2015 CSC 46, [2015] 3 R.C.S. 250 (aussi examinée pour un autre motif); *R. c. Chehil*, 2013 CSC 49, [2013] 3 R.C.S. 220 (aussi appliquée pour un autre motif); *R. c. Kang-Brown*, 2008 CSC 18, [2008] 1 R.C.S. 456 (aussi appliquée pour un autre motif).

DÉCISIONS EXAMINÉES :

Loi sur le Service canadien du renseignement de sécurité (Re), 2008 CF 300, [2008] 3 R.C.F. 477; *Canada (Citoyenneté et Immigration) c. Harkat*, 2014 CSC 37, [2014] 2 R.C.S. 33; *Ruby c. Canada (Solliciteur général)*, 2002 CSC 75, [2002] 4 R.C.S. 3; *R. v. Brewster*, 2016 ONSC 4133 (CanLII); *R. c. A.M.*, 2008 CSC 19, [2008] 1 R.C.S. 569 (aussi différenciée pour un autre motif); *R. c. Jarvis*, 2002 CSC 73, [2002] 3 R.C.S. 757; *R. c. Rodgers*, 2006 CSC 15, [2006] 1 R.C.S. 554; *Goodwin c. Colombie-Britannique (Superintendent of Motor Vehicles)*, 2015 CSC 46, [2015] 3 R.C.S. 250 (aussi différenciée pour un autre motif); *Mahjoub (Re)*, 2013 CF 1096; *Hypothèques Trustco Canada c. Canada*, 2005 CSC 54, [2005] 2 R.C.S. 602; *Mahjoub c. Canada (Citoyenneté et Immigration)*, 2017 CAF 157; *Charkaoui c. Canada (Citoyenneté et Immigration)*, 2007 CSC 9, [2007] 1

2007 SCC 9, [2007] 1 S.C.R. 350; *R. v. Nova Scotia Pharmaceutical Society*, [1992] 2 S.C.R. 606, (1992), 114 N.S.R. (2d) 91.

REFERRED TO:

R. v. McKinlay Transport Ltd., [1990] 1 S.C.R. 627, (1990), 68 D.L.R. (4th) 568; *R. v. Evans*, [1996] 1 S.C.R. 8, (1996), 131 D.L.R. (4th) 654; *R. v. Colarusso*, [1994] 1 S.C.R. 20, (1994), 110 D.L.R. (4th) 297; *R. v. Wholesale Travel Group Inc*, [1991] 3 S.C.R. 154 (1991), 84 D.L.R. (4th) 161; *R. v. Tse*, 2012 SCC 16, [2012] 1 S.C.R. 531; *Wakeling v. United States of America*, 2014 SCC 72, [2014] 3 S.C.R. 549; *R. v. Collins*, [1987] 1 S.C.R. 265, (1987), 38 D.L.R. (4th) 508;); *Charkaoui v. Canada (Citizenship and Immigration)*, 2008 SCC 38, [2008] 2 S.C.R. 326; *Comité paritaire de l'industrie de la chemise v. Potash; Comité paritaire de l'industrie de la chemise v. Sélection Milton*, [1994] 2 S.C.R. 406, (1994), 115 D.L.R. (4th) 702; *R. v. Simmons*, [1988] 2 S.C.R. 495, (1988), 55 D.L.R. (4th) 673; *R. v. Monney*, [1999] 1 S.C.R. 652, (1999), 171 D.L.R. (4th) 1; *R. v. M. (M.R.)*, [1998] 3 S.C.R. 393, (1998), 166 D.L.R. (4th) 261; *R. v. Grant*, [1993] 3 S.C.R. 223, [1993] 8 W.W.R. 257; *R. v. Mann*, 2004 SCC 52, [2004] 3 S.C.R. 59.

AUTHORS CITED

Canada. Parliament. Senate. Report of the Special Committee of the Senate on the Canadian Security Intelligence Service, *Delicate Balance: A Security Intelligence Service in a Democratic Society*. Ottawa: Supply and Services Canada (November 1983) (Chair: P. M Pitfield).

"RCMP, CSIS launch investigations into phone spying on Parliament Hill after CBC story", *CBC News* (April 4, 2017), online: < www.cbc.ca >.

"Spies' use of cellphone surveillance technology suspended in January, pending review", *CBC News* (May 3, 2017), online: < www.cbc.ca >.

Tamir Israel and 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.

Wikipedia – The Free Encyclopedia. "International mobile subscriber identity", online: https://en.wikipedia.org/wiki/International_mobile_subscriber_identity.

REFERENCE seeking to determine whether the Canadian Security Intelligence Service's warrantless use of CSS technology to capture the indentifying characteristics from the mobile devices of a known subject

R.C.S. 350; *R. c. Nova Scotia Pharmaceutical Society*, [1992] 2 R.C.S. 606.

DÉCISIONS CITÉES

R. c. McKinlay Transport Ltd., [1990] 1 R.C.S. 627; *R. c. Evans*, [1996] 1 R.C.S. 8; *R. c. Colarusso*, [1994] 1 R.C.S. 20; *R. c. Wholesale Travel Group Inc*, [1991] 3 R.C.S. 154; *R. c. Tse*, 2012 CSC 16, [2012] 1 R.C.S. 531; *Wakeling c. États-Unis d'Amérique*, 2014 CSC 72, [2014] 3 R.C.S. 549; *R. c. Collins*, [1987] 1 R.C.S. 265; *Charkaoui c. Canada (Citoyenneté et Immigration)*, 2008 CSC 38, [2008] 2 R.C.S. 326; *Comité paritaire de l'industrie de la chemise c. Potash; Comité paritaire de l'industrie de la chemise c. Sélection Milton*, [1994] 2 S.C.R. 406; *R. c. Simmons*, [1988] 2 R.C.S. 495; *R. c. Monney*, [1999] 1 R.C.S. 652; *R. c. M. (M.R.)*, [1998] 3 R.C.S. 393; *R. c. Grant*, [1993] 3 R.C.S. 223; *R. c. Mann*, 2004 CSC 52, [2004] 3 R.C.S. 59.

DOCTRINE CITÉE

Canada. Parlement. Sénat. Rapport du comité sénatorial spécial du Service canadien du renseignement de sécurité, *Équilibre délicat : Un Service du renseignement de sécurité dans une société démocratique.* Ottawa : Approvisionnements et Services Canada (novembre 1983) (Président : P. M Pitfield).

"RCMP, CSIS launch investigations into phone spying on Parliament Hill after CBC story", *CBC News* (4 avril 2017), en ligne : < www.cbc.ca >.

"Spies' use of cellphone surveillance technology suspended in January, pending review", *CBC News* (3 mai 2017), en ligne : < www.cbc.ca >.

Tamir Israel and 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.

Wikipedia – The Free Encyclopedia. "International Mobile Subscriber Identity", en ligne : https ://en.wikipedia.org/wiki/International_Mobile_Subscriber_Identity

RENVOI visant à déterminer si l'utilisation sans mandat par le Service canadien du renseignement de sécurité de la technologie relative aux ESB pour obtenir les caractéristiques distinctives des appareils

of investigation was unlawful. Judgment: Such use was not unlawful.

APPEARANCES

Jennifer Poirier, *Stéphanie Dion* and *Ilana Bleichert* for Department of Justice, National Security Litigation and Advisory Group.
Gordon Cameron and *Owen M. Rees* as *amici curiae*.

SOLICITORS OF RECORD

Deputy Attorney General of Canada for Department of Justice, National Security Litigation and Advisory Group.

The following are the public reasons for judgment and judgment rendered in English by

Crampton C.J.:

TABLE OF CONTENTS

mobiles de la cible connue d'une enquête était illégale. Jugement : L'utilisation en question n'était pas illégale.

ONT COMPARU :

Jennifer Poirier, *Stéphanie Dion* et *Ilana Bleichert* pour le ministère de la Justice, Groupe Litiges et conseils en sécurité nationale.
Gordon Cameron et *Owen M. Rees* en qualité d'*amici curiae*.

AVOCATS INSCRITS AU DOSSIER

Le sous-procureur général du Canada pour le ministère de la Justice, Groupe Litiges et conseils en sécurité nationale.

Voici les motifs publics du jugement et le jugement rendus en français par

Le juge en chef Crampton :

TABLE DES MATIÈRES

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*, being Part I of the *Constitution Act, 1982*, Schedule B, *Canada Act 1982*, 1982, c. 11 (U.K.) [R.S.C., 1985, Appendix II, No. 44] (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.

I. Introduction

[1] Dans une société libre et démocratique, il est attendu que les citoyens ne veulent pas que quiconque obtienne subrepticement les caractéristiques distinctives de leurs téléphones mobiles, y compris le Service canadien du renseignement de sécurité (SCRS ou Service) en vue de constituer un profil les concernant.

[2] Toutefois, le SCRS est libre de mener de telles activités dans les limites de la légalité et conformément aux paramètres établis dans sa loi habilitante et dans la *Charte canadienne des droits et libertés*, qui constitue la partie I de la *Loi constitutionnelle de 1982*, annexe B, *Loi de 1982 sur le Canada*, 1982, ch. 11 (R.-U.) [L.R.C. (1985), appendice II, no 44] (Charte). En l'espèce, la Cour doit se prononcer sur la légalité de l'activité qu'a menée le SCRS pour tirer de telles informations des appareils mobiles d'une cible connue, [***] Cette activité comprenait l'utilisation d'un émulateur de station de base (ESB) pour obtenir les caractéristiques distinctives des appareils mobiles de [***], et ce, sans mandat.

[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 [***] 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*, R.S.C., 1985, c. R-2, the *Criminal Code*, R.S.C., 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 [***] Furthermore, CSS technology should not be used to geo-locate anyone without a warrant.

[6] CSIS's use of a CSS against [***] constituted a "search" within the meaning of section 8 of the Charter. This is because [***] 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

[3] Les caractéristiques distinctives en question sont l'identité internationale de l'abonné mobile (*International Mobile Subscriber Identity* ou IMSI) et l'identité internationale d'équipement mobile (*International Mobile Equipment Identity* ou IMEI), des numéros émis par les appareils mobiles de [***] lorsqu'ils ont tenté de communiquer avec le réseau cellulaire de son fournisseur de services de télécommunication (FST). L'IMSI a indiqué le pays où se trouvait le compte de téléphonie cellulaire auquel était abonné [***] le code de réseau de son FST et le numéro d'identification unique que lui avait attribué le FST. L'IMEI a précisé la marque, le modèle et le numéro de série de l'appareil mobile.

[4] À mon avis, le SCRS n'a pas agi dans l'illégalité quand il a utilisé un ESB sans mandat dans le seul but d'obtenir les caractéristiques distinctives des appareils mobiles de [***] parce qu'il a pris un certain nombre de mesures pour s'assurer que l'activité était minimalement envahissante. Tant qu'il prendra des mesures similaires, le SCRS mènera en toute légalité des opérations fondées sur des ESB. Autrement dit, ces opérations ne contreviendront pas à la *Loi sur la radiocommunication*, L.R.C. (1985), ch. R-2, au *Code criminel*, L.R.C. (1985), ch. C-46 ni à la Charte.

[5] Entre autres, les mesures adoptées par le SCRS doivent limiter strictement son empiètement sur les droits en matière de vie privée de ses cibles et assurer que le Service ne recueille ni le contenu des communications effectuées à l'aide des appareils mobiles de quiconque, ni les données qui y sont stockées, ni les contenus auxquels ils permettent d'accéder. Les mesures doivent aussi assurer que les informations ayant trait aux appareils mobiles de tiers, recueillies fortuitement, sont détruites rapidement et ne font l'objet d'aucune analyse lorsqu'il a été confirmé que ces appareils mobiles ne sont pas ceux qu'utilise la cible [***] De plus, la technologie relative aux ESB ne doit pas servir à géolocaliser quiconque sans mandat.

[6] L'utilisation d'un ESB par le SCRS contre [***] a constitué une « fouille » au sens de l'article 8 de la Charte. Ma conclusion repose sur l'attente raisonnable en matière de vie privée de [***] relativement aux informations que le SCRS, en ayant accès aux IMSI et

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 [***] including by potentially helping CSIS to determine his [***] 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 [***] core biographic personal information, it engaged his rights under section 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 [***] 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

aux IMEI de ses appareils mobiles, pouvait commencer à recueillir à son endroit ou pouvait utiliser pour tirer des inférences plus fondées. En bref, à l'aide des informations dont il disposait déjà, ces numéros ont aidé le Service à esquisser le profil de [***] notamment en lui permettant éventuellement de mieux connaitre ses [***] et ses habitudes de communication. Dans la mesure où ceci a permis au SCRS de mieux comprendre certains aspects des renseignements biographiques d'ordre personnel de [***] ou de tirer des inférences plus fondées à leur égard, cette activité implique les droits qui lui sont garantis par l'article 8 de la Charte.

[7] Néanmoins, il ne s'agissait pas d'une fouille abusive, parce qu'elle était très ciblée, très précise et minimalement envahissante. Les opérations du SCRS fondées sur des ESB ont été encore moins envahissantes en ce qui a trait aux informations recueillies fortuitement qui provenaient d'appareils sans fil de tiers, celles-ci ayant été détruites rapidement et n'ayant fait l'objet d'aucune analyse après qu'il a été confirmé qu'elles ne concernaient pas les appareils sans fil de [***]

[8] De façon plus générale, en l'espèce, la preuve démontre que la technologie relative aux ESB utilisée par le SCRS ne lui permet ni d'établir l'identité de la personne dont les appareils mobiles sont visés par l'opération fondée sur des ESB, ni d'accéder aux informations sur la facturation ou à d'autres informations privées. En fait, en général, au moment d'utiliser les ESB, le SCRS connaît l'identité de la cible, sait où elle se trouve et dispose d'autres informations. Le Service a besoin d'un mandat pour obtenir des informations détaillées sur la facturation ou sur l'abonné auprès d'un FST, et ce, en raison de leur nature hautement privée. En effet, elles peuvent comprendre la liste de tous les appels effectués pendant la période de facturation, la durée de ces appels et le lieu où se trouvent les interlocuteurs.

[9] Les agents de l'État qui sont chargés de la sécurité du grand public peuvent mener des activités minimalement envahissantes sans enfreindre l'article 8 de la Charte, tant que ces activités sont autorisées par la loi, que les mesures législatives les autorisant sont raisonnables et que les activités n'ont pas été effectuées de manière abusive. À titre d'exemple, ils peuvent prendre

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*, R.S.C., 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, [2017] 2 F.C.R. 396 (*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 [***] CSIS gradually increased its use of the technology to the point that it has now been used across the country, [***]

[12] According to SIRC's report and the evidence provided in this proceeding, CSIS currently only uses CSS technology for two purposes, which are described in greater detail in Part V of these reasons below. The first such purpose is to attribute a cellular device to a subject of investigation whose identity is often already known. This was the case with [***] Such attribution is done by

une personne en filature dans un lieu public ou mesurer la quantité de chaleur qui émane de son domicile. En l'espèce, l'article 12 de la *Loi sur le Service canadien du renseignement de sécurité*, L.R.C. (1985), ch. C-23 (Loi sur le SCRS) autorise le Service à utiliser la technologie relative aux ESB. L'article 12 est une disposition législative raisonnable, et le SCRS a procédé à la fouille d'une manière raisonnable.

II. Contexte

[10] Il s'agit de la première fois que le SCRS demande explicitement l'avis de la Cour sur son utilisation de la technologie relative aux ESB pour obtenir, sans mandat, des informations ou des renseignements dans le cadre d'une enquête.

[11] Le SCRS utilise à cette fin la technologie relative aux ESB depuis plusieurs années. Toutefois, avant le 10 février 2016, la Cour ignorait cet état de fait. C'est à cette date que le SCRS lui a remis une copie du rapport classifié du Comité de surveillance des activités de renseignement de sécurité (CSARS) intitulé Étude du CSARS nº 2014-04 : *L'utilisation des métadonnées au SCRS*. Entre autres, le rapport traitait de deux études de cas. La première, [TRADUCTION] « Utilisation des métadonnées par le Centre d'analyse des données opérationnelles (CADO) », a mené mon collègue, le juge Simon Noël, à rendre une décision sur le programme de collecte et de conservation de telles informations par le SCRS (*X (Re)*, 2016 CF 1105, [2017] 2 R.C.F. 396 (*X (Re)*). L'autre, [TRADUCTION] « Collecte de l'identité internationale de l'abonné mobile (IMSI) par le Service », donnait un aperçu de l'utilisation de la technologie relative aux ESB par le SCRS au fil du temps. En bref, après avoir appris l'existence de cette technologie [***] le SCRS l'a utilisée de plus en plus, au point où il s'en sert maintenant d'un océan à l'autre, [***]

[12] Selon le rapport du CSARS et la preuve produite au cours de l'instance, le SCRS n'utilise actuellement la technologie relative aux ESB qu'à deux fins qui font l'objet de la partie V des présents motifs. En premier lieu, elle sert à attribuer un appareil cellulaire à une cible dont l'identité, souvent, est déjà connue; c'est ce qui s'est produit dans l'affaire impliquant [***] Pour ce

obtaining, through CSS technology, the IMSI associated with a subject of investigation's SIM [subscriber identity module] card, as well as the IMEI that is associated with a specific mobile device. Based on the information available to SIRC at the time it prepared its report, SIRC concluded that this activity alone does not require a warrant from this Court. However, SIRC added that any change to the uses of the information captured by the use of CSS technology would require further legal consideration.

[13] The second use that CSIS makes of CSS technology is to "geo-locate" a subject of investigation's cellular device. SIRC observed, and CSIS has since conceded, that this use of CSS technology must be sanctioned by a warrant issued by this Court.

[14] Before receiving SIRC's report in February 2016, Justice Mosley inquired about CSIS's use of the "Stingray" technology in the context of an *ex parte* hearing that took place on [***] and that concerned proposed changes to the template language of certain of this Court's warrants. However, CSIS's legal counsel was not in a position to provide a response to his general inquiry at that time.

[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 [***]

faire, le SCRS utilise la technologie relative aux ESB pour obtenir l'IMSI liée à la carte SIM [*subscriber identity module*, ou module d'identité d'abonné] de la cible ainsi que l'IMEI liée à un appareil mobile. Se fondant sur les informations auxquelles il avait accès au moment de préparer son rapport, le CSARS a conclu que cette activité en elle-même ne nécessite pas de mandat de la Cour. Il a toutefois ajouté qu'il y aurait lieu de soumettre à un examen juridique tout changement à l'utilisation des informations obtenues au moyen de cette technologie.

[13] En second lieu, le SCRS utilise la technologie relative aux ESB pour géolocaliser l'appareil cellulaire de la cible. Le CSARS a fait remarquer que cette utilisation doit être autorisée par un mandat décerné par la Cour, ce que le SCRS a reconnu depuis.

[14] Avant de recevoir le rapport du CSARS en février 2016, le juge Mosley s'était renseigné sur l'utilisation de la technologie « Stingray » par le SCRS lors d'une audience ex parte tenue le [***] qui portait sur des modifications proposées au libellé des modèles de certains mandats de la Cour. Cependant, à ce moment, l'avocat du SCRS n'était pas en mesure de fournir une réponse à cette question de nature générale.

[15] Peu après avoir eu l'occasion d'examiner le rapport du CSARS susmentionné, le juge Mosley a de nouveau posé des questions sur l'utilisation de la technologie relative aux ESB. Lors de cette audience [***] le déposant a témoigné que cette technologie avait été utilisée au cours de l'enquête qui avait mené à la demande de mandat et a expliqué de quelle manière elle l'avait été. Le déposant s'est engagé à confirmer que le SCRS détruit les données provenant d'appareils mobiles de tiers qu'il recueille au cours d'une opération fondée sur des ESB. Cette confirmation a finalement été apportée le [***] par [***] un employé de niveau supérieur du SCRS, à l'audition de la preuve relative à la présente demande.

[16] Le [***] lors de l'audition d'une autre demande [***] le juge Mosley a posé une question semblable à laquelle un autre déposant a donné une réponse semblable.

[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.[i] 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 similar technology, in exchanges between the Court and CSIS or its counsel. At the end of that letter, the Court was informed that [***] This was the first time that the Court had been informed that CSIS was using CSS or similar technology pursuant to its warrants.

[19] [***]

[***]

[***]

[20] On [***] 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 [***] 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.

[i] Justice Noël is the Coordinator of the Court's Designated Proceedings Unit.

[17] Par la suite, lors d'une conférence de gestion d'instance [***] que j'ai coprésidée le [***] avec le juge Noël, ce dernier a posé des questions sur la technologie « Stingray », sur son fonctionnement et sur son utilisation éventuelle dans l'exécution des mandats décernés par la Cour[i]. M. Jeff Yaworski, sous-directeur des Opérations (SDO) du SCRS, s'est engagé à fournir à la Cour les informations permettant de répondre aux questions du juge Noël. Ce n'est qu'après avoir pris connaissance des informations ensuite fournies par le SCRS que la Cour a commencé à bien comprendre la nature et la portée de l'utilisation de la technologie relative aux ESB par le SCRS.

[18] Le [***] dans une lettre adressée à la Cour, un avocat du SCRS a confirmé que les ESB ou des technologies similaires avaient uniquement été invoqués dans les échanges entre la Cour et le SCRS ou ses avocats dans le cadre des instances susmentionnées. À la fin de la lettre, le SCRS a informé la Cour que [TRADUCTION] [***] Ainsi, la Cour a appris que le SCRS utilisait des ESB ou des technologies similaires dans l'exécution de ses mandats.

[19] [***]

[***]

[***]

[20] Le [***] le juge Noël a émis une directive à l'endroit du SCRS et de la procureure générale pour qu'ils [TRADUCTION] « fournissent des informations et des éléments de preuve concernant la nature, la portée, l'utilisation et la minimisation de la technique d'enquête appelée "Stingray" ». Le juge Noël a ajouté que [TRADUCTION] « la Cour a besoin des informations et des éléments de preuve pour comprendre parfaitement la technique d'enquête et pour évaluer si le [***] ou tout autre mandat accorde le pouvoir légitime d'y recourir ». En fin de compte, le SCRS a décidé de fournir ces informations et éléments de preuve dans le cadre de la présente instance.

[i] Le juge Noël coordonne les Procédures désignées de la Cour.

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 [***] in connection with Islamist terrorism. As explained below, I granted those warrants with two amendments, for the period commencing on [***] and ending on [***]

[22] [***]

[23] The IMSI and IMEI numbers that were obtained from [***] wireless devices in [***] assisted CSIS to execute interception powers that this Court authorized in [***] 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 [***] affidavit) and [***] 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] [***]

[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 [***] in respect of [***] and that had been scheduled to expire on [***] The first exception was that I included language which prohibits the use of CSS [***] in paragraph [***] warrant. That prohibition has been included in several other warrants since the Court learned that CSIS had been relying on paragraph [***] in using CSS [***] 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 [***]

III. La présente instance

[21] Dans le cadre de la présente instance, le SCRS a demandé à la Cour de lui décerner des mandats en vertu des articles 12 et 21 de la Loi sur le SCRS pour lui permettre de poursuivre son enquête sur les activités liées au terrorisme islamiste que mène [***] Comme je l'explique plus loin, j'ai décerné les mandats en question, avec deux modifications, pour la période du [***] au [***]

[22] [***]

[23] Les IMSI et les IMEI obtenues des appareils sans fil de [***] en [***] ont aidé le SCRS à exercer les pouvoirs d'interception accordés par la Cour en [***] [***] contre les appareils sans fil expressément visés par les mandats décernés par la Cour.

[24] En appui à sa demande de mandat en l'espèce, le SCRS a présenté deux affidavits, ceux de [***] (affidavit [***] et de [***] (affidavit [***]. En outre, le SCRS et les *amici* ont présenté des documents, dont les réponses à des engagements pris avec moi en cours d'instance. Ces documents constituent des pièces.

[25] [***]

[26] À deux exceptions près, le libellé des mandats décernés dans le cadre de la présente instance était identique à celui des mandats qui avaient été décernés par le juge [***] contre [***] qui devaient expirer [***] En premier lieu, j'ai ajouté un passage interdisant le recours aux ESB [***] au paragraphe [***] du mandat [***] Cette interdiction a été ajoutée à plusieurs autres mandats depuis que la Cour a appris que le SCRS s'appuyait sur le paragraphe [***] pour utiliser les ESB et [***] contre des cibles de mandats décernés par la Cour. J'ai bien précisé au SCRS et à la procureure générale que cette modification ne signifiait pas que la Cour se prononçait sur la légalité de la technologie relative aux ESB, qu'elle soit utilisée en vertu d'un mandat ou sans mandat, car ces questions n'ont pas encore été réglées dans le cadre de la présente demande [***]

[27] The second amendment that I made to the warrant powers sought in this proceeding was to delete the requested authorization to obtain [***] That amendment was made after I determined that the evidence adduced by CSIS did not establish reasonable grounds to believe that [***]

[28] On [***] 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 [***] 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 [***] which included considerable information obtained in the course of CSIS's investigation of Islamist terrorism as well as more specific information concerning [***] That information was obtained through various methods of investigation, including physical surveillance and warranted intercepts involving [***] 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

[27] La seconde modification que j'ai apportée aux mandats demandés en l'espèce a été d'éliminer l'autorisation demandée d'obtenir des [***] J'ai pris cette mesure après avoir déterminé que les éléments de preuve présentés par le SCRS ne permettaient pas d'établir des motifs raisonnables de croire que [***]

[28] Le [***] à la fin de l'audition de la preuve en l'espèce, j'ai décerné au SCRS les mandats demandés, avec les modifications susmentionnées, et ce, après avoir acquis la conviction que le SCRS avait notamment démontré qu'il existait des motifs raisonnables de croire que les activités de [***] représentaient une « menace envers la sécurité du Canada », au sens de l'alinéa c) de la définition qui est donnée de cette expression à l'article 2 de la Loi sur le SCRS, et que les mandats étaient nécessaires pour enquêter sur cette menace.

[29] J'ai fondé ma décision sur les éléments de preuve fournis par [***] qui faisaient état d'une très grande quantité d'informations obtenues au cours de l'enquête du SCRS sur le terrorisme islamiste ainsi que d'informations concernant particulièrement [***] Pour les obtenir, le SCRS a utilisé différentes méthodes d'enquête, dont la filature et la réalisation d'interceptions en vertu de mandats contre [***] D'autres informations ont été obtenues auprès de sources humaines, au cours d'entrevues, grâce à des recherches dans les sources ouvertes ainsi qu'auprès d'organismes gouvernementaux au Canada et de services étrangers qui enquêtent aussi sur le terrorisme islamiste. Je ne me suis pas appuyé sur le peu d'informations obtenues sans mandat par le SCRS au moyen de la technologie relative aux ESB eu égard à [***] Ces informations ont été recueillies pendant deux jours et consistent uniquement en l'attribution de trois appareils à [***] à savoir [***] Selon l'un des déposants dans cette affaire, ces informations ont été détruites. Pour plus de précision, de plus, je ne me suis pas appuyer sur les informations découlant des numéros des IMSI et des numéros des IMEI obtenus au moyen de la technologie relative aux ESB, dont les communications effectuées au moyen de ces appareils que le SCRS a interceptées par la suite.

[30] En décernant les derniers mandats contre [***] j'ai bien précisé que je restais saisi de la demande afin

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 [***] including on cross-examination by the *amici*. I also considered it to be important that they have the benefit of responses provided by [***] 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 [***] 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.

i) de prendre note des modifications aux modèles des mandats découlant de la décision rendue par le juge Noël le 4 octobre 2016 dans *X (Re)*, ii) d'apporter les modifications correspondantes aux mandats que j'ai décernés provisoirement en l'espèce et iii) d'apporter aux mandats toute autre modification que je juge nécessaire après avoir eu l'occasion de prendre en considération les représentations légales soumises en cours d'instance.

[31] Parallèlement, par souci d'exhaustivité, il est utile de souligner que, dans une lettre datée du [***] la procureure générale a confirmé que le libellé du [***] a uniquement été invoqué dans [***] instances, soit [***] opérations de géolocalisation effectuées au moyen d'ESB. Elle a ajouté que, par le passé, le SCRS ne s'est fondé sur aucun mandat décerné par la Cour pour effectuer ses opérations au moyen d'ESB, car il estime ne pas avoir besoin d'un mandat pour recueillir des IMSI et des IMEI en vue d'attribuer un appareil à une cible.

[32] L'instance a fait l'objet de séances plénières parce qu'il s'agit de la première demande présentée à la Cour dans laquelle le SCRS i) a énoncé explicitement avoir utilisé la technologie relative aux ESB pour enquêter sur les activités d'une cible, ii) a présenté des observations sur la légalité du recours à cette technique dans le cadre de l'enquête et iii) a fourni des éléments de preuve relatifs à l'utilisation de cette technologie. J'ai estimé qu'il était utile d'inviter les autres juges désignés de la Cour à siéger avec moi afin qu'ils puissent prendre connaissance des éléments de preuve fournis par [***] notamment lors du contre-interrogatoire par les *amici*. À mon avis, il était aussi important qu'ils profitent des réponses de [***] à leurs questions ou aux miennes. Cela devrait aider chacun d'eux à traiter les futures demandes ayant trait à la technologie relative aux ESB, sans compter qu'il pourrait être moins nécessaire d'y présenter des éléments de preuve similaires.

[33] Le [***] en conclusion de l'audience, j'ai assuré le SCRS et les représentants de la procureure générale que la présence d'autres juges désignés en cours d'instance ne compromettait en rien mon indépendance judiciaire. Moi seul me suis prononcé sur les questions soulevées en l'espèce.

[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 [***] 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 [***] 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 [***] 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, R.S.C., 1985, c. C-23

Hearing of applications

27 An application under section 21, 21.1 or 23 for a warrant, an application under section 22 or 22.1 for the

[34] Compte tenu de l'importance des questions juridiques soulevées en l'espèce, la Cour a demandé à M. Gordon Cameron et à M. Owen Rees d'agir à titre d'*amici curiae*.

IV. Question préliminaire sur la publicité de l'audition des observations

[35] Le [***] lors de l'audition de la preuve, j'ai appris qu'il existait dans la sphère publique davantage d'informations sur la technologie relative aux ESB et sur son utilisation par les organismes d'application de la loi que ce que j'imaginais. Considérant cela ainsi que l'accroissement récent de l'intérêt du grand public envers la supervision des activités du SCRS par la Cour, j'ai demandé à la procureure générale si, à son avis, il était nécessaire que l'audition des observations relatives à cette technologie se déroule à huis clos.

[36] L'avocate de la procureure générale s'est engagée à demander des directives et à en faire part à la Cour. Elle a toutefois fait remarquer que le SCRS serait probablement réticent à prendre part à une audience publique à ce propos, puisqu'il n'a jamais été reconnu publiquement qu'il fait usage de cette technologie.

[37] Dans une lettre datée du [***] la procureure générale a pris position : selon elle, l'audition publique des observations en l'espèce ne serait pas appropriée. En bref, elle a estimé que la tenue d'une audience publique contreviendrait à l'article 27 de la Loi sur le SCRS et pourrait être très préjudiciable aux intérêts du Canada en matière de sécurité nationale. Entre autres, la procureure générale a soutenu qu'une audience publique nuirait [***] Elle propose qu'en lieu et place d'une audience publique, une décision dûment caviardée soit publiée.

[38] Voici l'article 27 de la *Loi sur le SCRS :*

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

Audition des demandes

27 Une demande de mandat faite en vertu des articles 21, 21.1 ou 23, de renouvellement de mandat faite en vertu des

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.]

[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, [2008] 3 F.C.R. 477, at paragraph 34:

> Section 27 provides that applications for warrant "shall be heard in private" ("*huis clos*" in French). "Private" is defined as "[c]onfidential; 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: avec lexique anglais-français*, (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 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" (paragraph 47). Ultimately, Justice Noël concluded that the issues of law

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. [Soulignement ajouté.]

[39] La procureure générale a fondé sa position selon laquelle l'audition publique des observations en l'espèce contreviendrait explicitement à l'article 27 sur l'extrait suivant de la décision rendue par le juge Noël dans *Loi sur le Service canadien du renseignement de sécurité (Re)*, 2008 CF 300, [2008] 3 R.C.F. 477, au paragraphe 34.

> En vertu de l'article 27, la demande de mandat « est entendue à huis clos » (« *private* », dans la version anglaise). Par « *private* », on entend « *confidential; secret* » dans le *Black's Law Dictionary*, 8e éd., (Brian A. Garner, , St Paul : Thomson West, 2004), et par « *private* » et « huis clos » dans le *Dictionnaire de droit québécois et canadien : avec lexique anglais-français* (Hubert Reid, Montréal : Wilson & Lafleur, 1994), « une exception au principe de la publicité des débats, qui consiste à interdire au public l'accès à la salle d'audience ». Une fois de plus, la confidentialité d'une demande de mandat a pour but de garantir le secret des informations sensibles en général et l'exécution du mandat. La personne visée (cible) ne doit pas être présente ou ne doit pas être au courant de la demande de mandat; autrement, l'objet d'une telle demande n'a aucune utilité pratique. Le public ne doit pas avoir accès à l'information parce que celle-ci se rapporte à la sécurité nationale et que l'efficacité des méthodes et des activités du SCRS reposent sur le secret. Enfin, l'information fournie par des tiers est souvent communiquée à condition qu'elle ne soit pas divulguée. Si les mandats étaient l'objet d'un examen public, des informations sensibles seraient probablement divulguées consciemment ou par inadvertance. Ce qui empêcherait le SCRS d'être informé des menaces qui pèsent sur la sécurité du Canada, rendrait l'enquête inutile, serait dangereux pour les informateurs concernés et risquerait de mettre en péril les relations du Canada avec les pays alliés.

[40] Toutefois, la procureure générale n'a pas remarqué qu'au paragraphe 46 de sa décision, le juge Noël avait souligné que « les questions "incidentes" liées à une demande de mandat, notamment les questions de compétence, pourraient être examinées en audience publique dans certaines circonstances ». À cet égard, a insisté le juge Noël au paragraphe 47, « en gardant à l'esprit le libellé précis de l'article 27 de la Loi sur le SCRS et l'équilibre à maintenir entre la sécurité nationale et les droits fondamentaux, je crois que chaque cas est un

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>.)

cas d'espèce». Le juge Noël a conclu que, dans l'affaire dont il était saisi, les questions de droit et de faits étaient si étroitement liées que la question de compétence qui avait été soulevée ne pouvait pas être réglée en public.

[41] En l'espèce, d'emblée, il ne m'est pas apparu évident que les questions de droit et de faits étaient aussi étroitement liées. Toutefois, il a été su plus tard que la preuve factuelle qui a été présentée a été essentielle aux conclusions auxquelles j'en suis arrivé pour déterminer si l'utilisation de la technologie relative aux ESB par le SCRS constituait une fouille et si cette fouille était abusive au sens de l'article 8 de la Charte.

[42] Les motifs invoqués par la procureure générale pour s'opposer à la tenue d'une audience publique ont été grandement ébranlés par deux éléments importants qui ont surgi entre l'audition de la preuve et l'audition des observations des parties. Premièrement, le ministre aurait confirmé publiquement que le SCRS et la Gendarmerie royale du Canada (GRC) utilisaient la technologie relative aux ESB, mais seulement [TRADUCTION] «dans le cadre législatif» («RCMP, CSIS launch investigations into phone spying on Parliament Hill after CBC story» (La GRC et le SCRS enquêtent sur l'espionnage des téléphones sur la Colline du Parlement à la suite d'un reportage de la CBC), *CBC News*, 4 avril 2017, en ligne : <www.cbc.ca>). La procureure générale a confirmé cet état de fait dans une lettre adressée à la Cour le 5 avril 2017, mais elle a maintenu que «l'audition des observations relatives à l'utilisation d'ESB par le SCRS doit se poursuivre à huis clos, conformément à l'article 27 de la [Loi sur le SCRS], pour éviter un grave préjudice aux intérêts en matière de sécurité nationale».

[43] L'autre élément important est la publication d'un reportage de la CBC la veille de l'audition des observations en l'espèce. Selon ce reportage, le SCRS aurait «confirmé avoir utilisé la technologie permettant de repérer et de suivre des téléphones cellulaires au cours des dernières années, avec et sans mandat» («Spies' use of cellphone surveillance technology suspended in January, pending review» (Depuis janvier, les espions ont cessé d'utiliser la technologie permettant de surveiller des téléphones cellulaires pendant que la question fait l'objet d'un examen), *CBC News*, 3 mai 2017, en ligne : <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, [2014] 2 S.C.R. 33 (*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 paragraph 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.

[44] Étant donné que le SCRS aurait confirmé qu'il utilisait la technologie relative aux ESB, les *amici* ont envoyé à la Cour une courte lettre laissant entendre que, partant, l'audition des observations en l'espèce devrait être publique. Tout en reconnaissant que l'article 27 exige que les demandes de mandats soient entendues à huis clos, ils ont fait remarquer que des déclarations de la Cour suprême du Canada dans l'arrêt *Canada (Citoyenneté et Immigration) c. Harkat*, 2014 CSC 37, [2014] 2 R.C.S. 33 (*Harkat*) appuieraient la décision de la Cour de tenir publiquement l'audition des observations sur l'utilisation d'ESB par le Service. Au paragraphe 25 de l'arrêt *Harkat*, la Cour suprême fait remarquer que les questions soulevées dans le dossier « ne port[aient] pas sur des renseignements confidentiels [et qu'elles] auraient donc pu être débattues totalement en public sans risque réel de divulgation, et [que] ces débats [auraient pu] être complétés, au besoin, de brèves observations confidentielles par écrit et du dossier confidentiel ». Au paragraphe 26, la Cour ajoute que la teneur de l'audience à huis clos ne l'a pas aidé à trancher les questions dont elle était saisie, et que l'audience à huis clos « n'a servi qu'à entretenir l'apparente opacité de l'instance, ce qui contrevient aux principes fondamentaux de transparence et de responsabilisation ». Les *amici* n'ont pas abordé les différences entre l'affaire dont était saisie la Cour suprême et la demande en l'espèce.

[45] Le même jour, en réaction à la suggestion des *amici*, la procureure générale a envoyé une courte lettre à la Cour dans laquelle elle a accepté de discuter de la possibilité de tenir une audience publique. Toutefois, elle a fait remarquer qu'un ajournement pourrait être nécessaire pour permettre de déterminer quels éléments seraient susceptibles de faire l'objet d'une audience publique et ceux qui devraient être étudiés à huis clos. En outre, elle a vivement recommandé de tenir compte de l'article 27 de la Loi sur le SCRS.

[46] Le lendemain matin, à la fin de l'audition des observations relatives à la présente demande, les *amici* ont de nouveau suggéré que la Cour ajourne l'audience pour leur permettre, de concert avec la procureure générale, de trouver une manière pour qu'au moins une partie des observations orales soient entendues en public.

[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, [2002] 4 S.C.R. 3, at paragraphs 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*, R.S.C., 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 paragraphs 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

[47] Toutefois, en raison du caractère tardif de la suggestion des *amici* ainsi que de l'absence d'autres observations de leur part et de celle de la procureure générale quant à la manière dont une audience publique pourrait être tenue, considérant le libellé précis de l'article 27, j'ai décidé de procéder comme prévu.

[48] J'ai pris cette décision sans perdre de vue l'arrêt *Ruby c. Canada (Solliciteur général)*, 2002 CSC 75, [2002] 4 R.C.S. 3 (*Ruby*), aux paragraphes 57 et 58, dans lequel la Cour suprême du Canada souligne qu'il n'est pas loisible aux parties, même si elles y consentent toutes, d'écarter les dispositions impératives de l'alinéa 51(2)a) de la *Loi sur la protection des renseignements personnels*, L.R.C. (1985), ch. P-21, qui portent sur le huis clos. La Cour suprême ajoute qu'à moins qu'il y ait un enjeu constitutionnel, il n'est pas non plus loisible au juge de tenir une audience publique et, de ce fait, de contrevenir directement à cette loi, même s'il ne s'agit que de points de droit, quoi que puissent proposer les parties à cet égard. (Plus loin, la Cour affirme que, pour des motifs de nature constitutionnelle, il y a lieu de donner une interprétation atténuante de certaines dispositions de la *Loi sur la protection des renseignements personnels* de façon à ce qu'elles ne s'appliquent qu'à certains types d'observations présentées *ex parte*, ce qui permet au tribunal de procéder à des parties de l'audition en audience publique. *Ruby*, précité, aux paragraphes 58 à 60.)

[49] J'ai aussi tenu compte du fait qu'en pratique, il aurait été difficile de réaffecter un nombre adéquat de juges désignés à une date quelconque avant octobre ou novembre de cette année. En outre, j'étais conscient du fait que la procureure générale avait déjà présenté ses observations à la Cour lorsque, pour la première fois, j'ai manifesté de l'intérêt envers la possibilité de tenir une audience publique pour entendre, en tout ou en partie, les observations orales en l'espèce. J'étais conscient que cela aurait été la première audience publique tenue dans le cadre d'une demande de mandat présentée en vertu de l'article 21 de la Loi sur le SCRS. Présumant que, dans certaines circonstances, l'article 27 n'interdit pas la tenue d'une audience publique, j'ai considéré qu'il serait préférable qu'une telle audience ait lieu dans le cadre d'une instance ayant fait l'objet d'une meilleure

the time I was not entirely convinced that the factual and legal issues were intimately linked. As I have already noted, it subsequently became apparent that they were indeed so linked.

[50] In the meantime, I considered it appropriate to considerably reduce the opacity that otherwise would be associated with this proceeding by issuing public redacted versions of both this decision and the written versions of the parties' arguments. In my view, those measures, taken together, will represent an important additional step by this Court to foster greater openness with respect to the *ex parte* proceedings that are brought before it under the Act. Stated differently, these measures will increase the principles of transparency and accountability to which the Supreme Court referred in *Harkat*, above, at paragraph 26.

V. CSS Technology

[51] Information regarding the manner in which the CSS technology functions was provided to the Court by [***] both through the [***] affidavit and orally during the evidentiary hearing on [***]

[52] [***] is employed by CSIS as a [***] He did not testify on what was done specifically in the case of [***] but rather spoke of the CSS technique generally. Among other things, he described himself as a subject-matter expert with respect to the CSS technology. [***] His evidence was provided for the purpose of assisting the Court to determine whether information obtained without a warrant that specifically sanctioned the use of a CSS, had been obtained lawfully and may be relied upon in an application by CSIS for warrants under section 21 of the Act.

[53] [***] explained that CSS is an umbrella term that encompasses both generic terms that are sometimes used, such as "IMSI grabber" or "IMSI catcher, as well as manufacturer or vendor-based names such as Stingray, [***]

[54] [***] confirmed that CSIS utilizes CSS technology solely for the two purposes that were previously

planification à cet égard. Enfin, à ce moment, je n'étais pas entièrement convaincu que les questions de faits et de droit étaient intimement liées. Comme je l'ai déjà souligné, il est ensuite devenu apparent que cela était bel et bien le cas.

[50] Entre-temps, il m'a semblé judicieux de réduire considérablement l'opacité qui entourerait normalement l'instance, c'est-à-dire de publier des versions caviardées de la présente décision et des observations écrites des parties. À mon avis, grâce à ces mesures, la Cour fera un grand pas vers une ouverture accrue relativement aux instances *ex parte* dont elle est saisie au titre de la Loi sur le SCRS. Autrement dit, ces mesures accroîtront la transparence et la responsabilisation, principes auxquels la Cour suprême a fait allusion dans l'arrêt *Harkat*, précité, au paragraphe 26.

V. Technologie relative aux ESB

[51] Les informations sur le fonctionnement de la technologie relative aux ESB ont été fournies à la Cour par [***] dans son affidavit et de vive voix le [***] lors de l'audition de la preuve.

[52] [***] est [***] au SCRS. Son témoignage ne traitait pas du cas de [***] en particulier, mais plutôt de la technique en général. Il se décrit entre autres comme un spécialiste de la technologie relative aux ESB. [***] Les éléments de preuve qu'il a fournis étaient destinés à aider la Cour à déterminer s'il était légal d'obtenir des informations sans qu'un mandat autorise précisément l'utilisation d'un ESB et si, partant, la Cour peut se fonder sur ces informations dans le cadre d'une demande de mandat présentée par le SCRS en vertu de l'article 21 de la Loi sur le SCRS.

[53] [***] a expliqué que le terme « ESB » est un générique qui englobe à la fois les termes parfois utilisés, comme « intercepteur d'IMSI » ou « capteur d'IMSI », et les appellations du fabricant ou du fournisseur, comme Stingray, [***]

[54] [***] a confirmé que le SCRS utilise la technologie relative aux ESB uniquement aux deux fins recensées

identified by SIRC, and discussed at paragraph 12 above, namely, (i) to attribute a cellular device to a known subject of investigation and, (ii) once attributed, to geo-locate a subject of investigation's cellular device at some later date, when the subject's precise whereabouts are no longer known by CSIS.

[55] [***] noted that, when CSIS uses a CSS for the first purpose, it already knows the location of the individual, but not the IMSI or IMEI of the individual's mobile device(s). In addition, the identity of the subject of investigation is also typically known. In describing this use of the CSS technology, [***] stated: "Our goal is to identify cellular devices and attribute them to subjects of investigation. This would be a clear investigative requirement in order to be able to determine [***] and communication patterns [***]

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

[57] According to [***] 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. [***] 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.

précédemment par le CSARS, et discuté ci-dessus au paragraphe 12, c'est-à-dire i) attribuer un appareil cellulaire à une cible connue et, une fois l'attribution effectuée, ii) géolocaliser l'appareil cellulaire de la cible à une date ultérieure, lorsque le SCRS ne saura plus exactement où se trouve cette dernière.

[55] [***] a souligné que, lorsqu'il utilise un ESB pour attribuer un appareil, le SCRS sait où se trouve la personne, mais ignore l'IMSI ou l'IMEI de ses appareils mobiles. En outre, il connaît habituellement l'identité de la cible. Lorsqu'il a décrit cette utilisation de la technologie relative aux ESB, [***] a déclaré que [TRADUCTION] « nous cherchons à reconnaître les appareils cellulaires et à les attribuer aux cibles. Aux fins de l'enquête, cela nous est manifestement nécessaire pour esquisser les [***] et les habitudes de communication [***]

[56] Comparativement aux faits qu'il connaît au moment de procéder à une opération fondée sur des ESB pour le motif susmentionné, le SCRS, lorsqu'il utilise un ESB pour géolocaliser une personne, connaît une ou plusieurs IMSI ou IMEI liées à cette personne, mais ne sait pas où elle se trouve. [***] a précisé que le SCRS ne cherche pas à géolocaliser quiconque sans mandat au moyen d'une opération fondée sur des ESB.

[57] Selon [***] les FST sont capables de reconnaître les appareils mobiles autorisés à accéder à leurs services grâce à deux éléments d'information uniques que ces appareils fournissent, c'est-à-dire l'IMSI et l'IMEI, que [***] a décrit ainsi dans son affidavit.

> [TRADUCTION]
>
> 13. L'IMSI est une série de 15 chiffres permettant d'établir un lien unique entre un compte d'abonné et un FST. Il comporte trois parties : l'indicatif du pays de l'abonné (*Mobile Country Code* ou MCC) à trois chiffres, le code de réseau local de l'abonné (*Mobile Network Code* ou MNC) à deux ou trois chiffres, le reste des chiffres constituant le numéro d'identification unique de l'abonné (*Mobile Subscriber Identification Number* ou MSIN) permettant au fournisseur de service de repérer le compte de l'utilisateur dans son système.

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, [***] 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, [***] 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] [***]

[61] [***]

[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. [***]

[63] [***]

[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] [***]

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

14. L'IMEI est une série de 15 chiffres permettant au FST de reconnaître l'appareil lui-même […]. Les huit premiers chiffres (*Type Allocation Code* ou TAC) renvoient à la marque et au modèle de l'appareil. Les sept autres chiffres constituent le numéro de série unique de l'appareil.

[58] [***] a proposé l'IMSI 302720123456789 à titre d'exemple. Dans ce numéro, le segment « 302 » représente l'indicatif de pays de l'abonné (MCC) et le segment « 720 » représente le code de réseau mobile (MNC) du FST. Les autres chiffres constituent le numéro d'identification unique de l'abonné (MSIN). Ces informations sont stockées sur la carte SIM de l'appareil mobile.

[59] En outre, toujours à titre d'exemple, [***] a proposé l'IMEI 353778081234560. Dans ce numéro, le segment « 35377808 » permet d'établir la marque et le modèle de l'appareil (TAC) tandis que la séquence « 1234560 » représente le numéro de série unique de l'appareil. Selon la compréhension de la Cour, ces informations sont stockées dans l'appareil lui-même, pas sur la carte SIM.

[60] [***]

[61] [***]

[62] Pour faciliter la prestation de services de télécommunication, chaque FST se voit attribuer des fréquences qui lui sont propres et sur lesquelles il peut diffuser et mener ses activités. [***]

[63] [***]

[64] Essentiellement, l'ESB imite une tour de téléphonie cellulaire d'un FST. Il amène ainsi les appareils cellulaires à interagir avec lui et à s'authentifier auprès de lui comme s'il était une tour véritable.

[65] [***]

[66] Pour pouvoir reconnaître l'IMSI et l'IMEI qui correspondent à l'appareil qu'utilise la cible de l'opération menée au moyen d'un ESB, [***]

[67] [***]

[68] [***]

[69] [***]

[70] [***]

[71] [***]

[72] [***] 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. [***]

[73] [***] 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. [***][ii] [***]

[74] Finally, [***] 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 [***] CSIS DDO issued a Directive relating to the collection and retention of electronic identifiers. According to [***] 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, [***]

[ii] [***] 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.

[67] [***]

[68] [***]

[69] [***]

[70] [***]

[71] [***]

[72] [***] le SCRS utilise les ESB d'une manière qui ne nuit d'aucune façon perceptible à la qualité du service dont bénéficient les utilisateurs d'appareils mobiles qui se trouvent à proximité. [***]

[73] [***] a en outre assuré la Cour qu'à une exception près, la technologie relative aux ESB utilisée par le SCRS ne permet aucunement de recueillir le contenu des communications des utilisateurs d'appareils mobiles ni les informations stockées sur les appareils. [***][ii][***]

[74] Enfin [***] a souligné que les IMEI et IMSI recueillies par les ESB ne sont pas cryptées et sont libres d'accès.

VI. Politique du SCRS sur la collecte et la conservation d'identificateurs électroniques

[75] Le [***] le SDO du SCRS a donné une directive sur la collecte et la conservation d'identificateurs électroniques. Selon [***] cette directive fait suite à la décision rendue par le juge Noël dans *X (Re)*, dans laquelle il a statué que l'expression « strictement nécessaire » qui figure à l'article 12 de la Loi sur le SCRS s'applique aussi bien à la collecte qu'à la conservation d'informations par le SCRS.

[76] Aux fins de la directive, s'entend par « identificateurs électroniques » l'IMSI, l'IMEI [***]

[ii] [***] a témoigné qu'il existe des technologies relatives aux ESB qui permettent d'intercepter le contenu d'appels téléphoniques, mais que le SCRS ne possède ni n'utilise aucun appareil de ce type. Je m'attends à ce que le SCRS présente une demande de mandat à la Cour s'il acquiert un jour une telle technologie, car il est manifeste que l'interception de ce genre de contenu nécessite préalablement une approbation judiciaire.

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

[78] According to [***] 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. [***]

[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. [***] testified that the operational reports are usually prepared "within [***] 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 [***] 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 paragraph 253, that "information that is evidently not threat-related and that does not involve the target" must be destroyed. [***]

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.

[77] Conformément à la directive, un moratoire a été imposé relativement à l'utilisation de moyens techniques servant à recueillir des identificateurs électroniques. [***]

[78] Selon [***] tous les identificateurs électroniques obtenus par le SCRS dans le cadre d'opérations fondées sur des ESB, y compris ceux qui ont fait l'objet d'un rapport opérationnel, ont été détruits conformément à la directive. [***]

[79] Ajoutons à ces informations contextuelles que, pendant l'audition de la preuve en l'espèce, la procureure générale a expliqué que les identificateurs sont généralement supprimés dès que le rapport opérationnel concernant l'activité de collecte a été rédigé, et ce, en raison de la décision du juge Noël dans *X (Re)* et de l'opinion du SCRS voulant que la conservation de l'IMSI et de l'IMEI ne saurait être, à ce moment, considérée comme « strictement nécessaire ». Selon [***] les rapports opérationnels sont généralement préparés dans [***] jours suivants. Il a toutefois ajouté que, lorsqu'il aura repris les opérations fondées sur des ESB après la publication des présents motifs, le SCRS envisage de demander une période maximale de [***] mois pour déterminer si les IMSI et les IMEI qu'il a recueillies peuvent être attribuées à une cible. Il s'agit de la période pour laquelle le juge Noël a déterminé dans la décision *X (Re)*, précitée, au paragraphe 253, que « les informations qui ne sont manifestement pas liées à la menace et qui n'impliquent pas la cible » doivent être détruites. [***]

VII. Évaluation des observations

[80] La procureure générale soutient que l'utilisation de la technologie relative aux ESB par le SCRS à la seule fin de recueillir des IMSI et des IMEI n'enfreint ni la *Loi sur la radiocommunication*, ni le *Code criminel*, ni la Charte. Je suis d'accord, pour les motifs ci-dessous.

[81] Les observations de la procureure générale ayant trait à chacune de ces lois sont abordées de façon distincte ci-dessous.

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, R.S.C. 1985, c. C-23.

A. *Loi sur la radiocommunication*

[82] La *Loi sur la radiocommunication* régit l'utilisation d'appareils radio et de matériel radiosensible pour assurer le développement ordonné et l'exploitation efficace de la radiocommunication au Canada. À cette fin, l'alinéa 5(1)a) de cette loi permet au ministre de l'Industrie (maintenant le ministre de l'Innovation, des Sciences et du Développement économique) de décerner les licences et les certificats régissant les appareils radio, dont « toute autre autorisation relative à la radiocommunication qu'il estime indiquée ».

[83] Entre autres, l'alinéa 9(1)b) de cette loi interdit, « sans excuse légitime, de gêner ou d'entraver la radiocommunication ».

[84] La procureure générale reconnaît qu'un ESB est un « appareil radio » au sens de la *Loi sur la radiocommunication*. Elle soutient toutefois que le SCRS l'utilise légalement, parce qu'il détient une autorisation relative à l'utilisation d'appareils radio (Autorisation) émise le 1er septembre 1992. Elle soutient en outre qu'au titre de l'Autorisation et de l'article 12 de la Loi sur le SCRS, l'utilisation que fait le SCRS de la technologie relative aux ESB ne contrevient pas à l'alinéa 9(1)b) de la *Loi sur la radiocommunication*.

[85] Aux fins des présents motifs, voici les dispositions les plus utiles de l'Autorisation.

> 1) Aux termes du sous-alinéa 5(1)a)(v) de la *Loi sur la radiocommunication*, la présente constitue une autorisation pour le Service canadien du renseignement de sécurité (SCRS) relativement à tous les types d'appareils radio spécialement conçus aux fins indiquées au paragraphe 2, à l'égard desquels une licence radio, délivrée en vertu du sous-alinéa 5(1)a)(i) de la *Loi sur la radiocommunication*, n'est pas indiquée.
>
> 2) La présente autorisation s'applique aux appareils radio décrits au paragraphe 1 seulement quand ils sont mis à l'essai ou quand ils sont utilisés à des fins de formation ou à des fins d'activités opérationnelles dans le cadre des enquêtes menées en vertu des articles 12 et 16 de la *Loi sur le Service canadien du renseignement de sécurité*, LRC (1985), ch 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 [***] 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.

[…]

7) Aucun appareil radio visé par la présente autorisation ne devra causer une interférence nuisible à d'autres appareils radio faisant l'objet d'une autorisation ou d'une licence.

[…]

9) La présente autorisation est valide à moins d'être retirée par le ministère des Communications ou à moins que le Service canadien du renseignement de sécurité (SCRS) indique par écrit qu'elle n'est plus nécessaire. [Non souligné dans l'original.]

[86] Le texte complet de l'Autorisation figure à l'annexe I des présents motifs.

[87] Les *amici* soulignent que le SCRS n'a pas eu accès à la technologie relative aux ESB [***] Ils soutiennent qu'il n'est pas raisonnablement concevable qu'en 1992, à l'aube de la technologie cellulaire, le ministre ait envisagé que l'Autorisation puisse être interprétée comme une permission d'utiliser du matériel en vue d'obtenir des IMSI et des IMEI. Selon eux, si le SCRS avait demandé l'autorisation au ministre actuel, celui-ci aurait vraisemblablement mis des balises à l'utilisation de la technologie relative aux ESB, comme il l'a fait dans l'autorisation délivrée le 13 mars 2017 à la GRC. Le texte complet de cette autorisation figure à l'annexe II des présents motifs.

[88] Les arguments susmentionnés sont peut-être empreints de vérité, mais ils ne tiennent pas compte du fait qu'à première vue, le libellé de l'Autorisation est assez général pour inclure l'utilisation d'ESB et du matériel connexe par le SCRS.

[89] En particulier, la portée du segment « relativement à tous les types d'appareils radio spécialement conçus aux fins indiquées au paragraphe 2 », qui figure au paragraphe 1 de l'Autorisation, englobe clairement l'utilisation de ce genre de matériel. Je suis enclin à me ranger à l'avis du SCRS, selon qui ce segment semble indiquer qu'il a été envisagé, lorsque l'Autorisation a été délivrée, qu'elle allait être invoquée à l'endroit d'appareils radio qui n'existaient pas en 1992.

[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 *Radiocommunication 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 Ac*t, R.S.C., 1985, c. R-2

Definitions

2 …

harmful interference … an adverse effect of electromagnetic energy from any emission, radiation or induction that

(a) endangers the use or functioning of a safety-related radiocommunication 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 (CanLII), at paragraphs 34, 38, 51–52. However, the passages from that decision that were cited by the *amici* simply described

[90] Quoi qu'il en soit, en raison de ce segment, l'Autorisation peut être invoquée à l'endroit de tels appareils radio. Comme il est prévu au paragraphe 9 de l'Autorisation, celle-ci suffit à permettre au SCRS, aux fins de la *Loi sur la radiocommunication*, d'utiliser des ESB et le matériel connexe, et ce, jusqu'à ce que le ministre la retire. Selon la preuve présentée en l'espèce, le ministre n'a pas entrepris une telle démarche.

[91] Je fais remarquer au passage que la procureure générale a souligné qu'avant d'obtenir l'autorisation susmentionnée en mars de cette année, la GRC s'appuyait sur une autorisation distincte, relative aux brouilleurs, pour mener ses opérations fondées sur des ESB.

[92] Les *amici* ont ajouté que l'utilisation d'un ESB pour obtenir des IMSI et des IMEI cause manifestement du brouillage à l'endroit des appareils cellulaires visés et est susceptible d'être la source de brouillage préjudiciable, au sens du paragraphe 7 de l'Autorisation. À ce propos, ils soulignent que la *Loi sur la radiocommunication* donne la définition suivante de «brouillage préjudiciable».

Loi sur la radiocommunication, L.R.C. (1985), ch. R-2

Définitions

2 […]

brouillage préjudiciable Effet non désiré d'une énergie électromagnétique due aux 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.

[93] Les *amici* soulignent en outre que la possibilité d'être à l'origine de brouillage préjudiciable, notamment à l'endroit des appels d'urgence adressés au 911, est un élément du dossier dont a été saisi le juge Code de la Cour supérieure de justice de l'Ontario dans la décision *R. v. Brewster*, 2016 ONSC 4133 (CanLII), aux paragraphes 34, 38, 51 et 52. Toutefois, les extraits de

(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 [***] In my view, [***] 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 [ss. 183 to 196.1] 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. [***]

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

Criminal Code, R.S.C., 1985, c. C-46

cette décision cités par les *amici* traitent simplement i) de mesures adoptées par la GRC relativement à la manipulation de *ses* ESB et du matériel connexe en vue de minimiser la possibilité de causer un brouillage préjudiciable à des téléphones mobiles, ii) de la capacité de *ce* matériel d'interrompre les appels pendant une durée maximale de deux minutes (lorsqu'il est configuré d'une manière rarement utilisée) et iii) d'arguments relatifs à des lacunes présumées aux mandats de la GRC qu'a rejetés le juge Code. En outre, il y a lieu de souligner que le juge Code a fondé ses observations sur la preuve qui avait été présentée lors de cette instance.

[94] En l'espèce, selon la preuve, le matériel utilisé par le SCRS [***] À mon avis, [***] ne constituent pas de sérieuses dégradations ou entraves ni des interruptions répétées, au sens de l'article 2 de la *Loi sur la radiocommunication* cité ci-dessus.

[95] Compte tenu de ce qui précède, je suis convaincu que l'utilisation que fait le SCRS de la technologie relative aux ESB ne contrevient pas à la *Loi sur la radiocommunication*.

B. *Code criminel*

[96] La Partie VI [articles 183 à 196.1] du *Code criminel* prévoit un régime régissant l'interception des communications privées. Entre autres, l'article 184 du *Code criminel* interdit d'intercepter volontairement une communication privée au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre en l'absence de consentement ou d'autorisation judiciaire.

[97] Le SCRS soutient qu'il n'a pas contrevenu à l'article 184 du *Code criminel* en utilisant des ESB et le matériel connexe sans avoir obtenu d'autorisation judiciaire au préalable parce que les appareils en question n'interceptent aucune communication privée. [***]

[98] L'article 183 du *Code criminel* donne la définition suivante de « communication privée ».

Code criminel, L.R.C. (1985), ch. C-46

Definitions

183 …

private communication … 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.

Définitions

183 […]

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.

[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.

[99] Toujours selon l'article 183 du *Code criminel*, « intercepter » « [s]'entend notamment du fait d'écouter, d'enregistrer ou de prendre volontairement connaissance d'une communication ou de sa substance, son sens ou son objet ». Le SCRS et les *amici* s'entendent pour dire que l'obtention d'IMSI et d'IMEI au moyen d'ESB ne saurait être assimilée à l'une de ces actions ni à la capture de tout contenu de communications effectuées au moyen des appareils mobiles visés.

[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*.

[100] Ainsi, les *amici* conviennent qu'en l'absence de toute interception du contenu de communications, l'utilisation que fait le SCRS de la technologie relative aux ESB en vue d'attribuer des IMSI et des IMEI à une cible ne contrevient pas à la Partie VI du *Code criminel*.

[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.

[101] Cependant, les *amici* ont soutenu que l'utilisation d'un ESB sans mandat par le SCRS enfreint les dispositions de l'article 430 du *Code criminel* sur les méfaits et que ni l'article 12 de la Loi sur le SCRS ni l'Autorisation dont il est question aux paragraphes 84 à 90 ci-haut ne fournissent d'exemptions légitimes à l'article 430. Je ne suis pas d'accord.

[102] Subsection 430(1) states:

[102] Voici le paragraphe 430(1).

Criminal Code, R.S.C., 1985, c. C-46

Code criminel, L.R.C. (1985), ch. C-46

Mischief

430 (1) Every one commits mischief who wilfully

Méfait

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

(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.

[103] Pursuant to section 429 of the *Criminal Code*, "[n]o 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

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] Aux termes de l'article 429 du *Code criminel*, « 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 ».

[104] Pour les raisons exposées à la Partie VII.A des présents motifs, je rejette la position des *amici*, selon qui l'autorisation ne procure pas une telle justification légale.

[105] Pour les raisons exposées à la Partie VII.C.(2)(b)(ii) des présents motifs, je rejette la position des *amici* à l'égard de l'article 12.

[106] J'ajoute simplement au passage que, dans leurs observations orales, les *amici* ont reconnu que, si je statue que l'article 12 suffit à autoriser la collecte de l'IMSI et de l'IMEI au moyen de la technologie relative aux ESB, cette activité pourrait être visée par une défense fondée sur l'article 429 du *Code criminel*.

C. Article 8 de la Charte

1) *Principes juridiques*

[107] Suivant l'article 8 de la Charte, « [c]hacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives ».

[108] Partant, deux questions distinctes doivent être étudiées pour déterminer s'il y a eu infraction à l'article 8 : i) la possibilité qu'il y ait eu une fouille, une perquisition ou une saisie et, dans l'affirmative ii), la possibilité qu'elle

seizure was "unreasonable", (*R. v. Gomboc*, 2010 SCC 55, [2010] 3 S.C.R. 211 (*Gomboc*), at paragraph 20).

[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, [2014] 2 S.C.R. 212 (*Spencer*),at paragraph 15).

(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 S.C.R. 425 (*Thomson Newspapers*), at page 505; *R. v. McKinlay Transport Ltd.*, [1990] 1 S.C.R. 627 (*McKinlay*), at page 642).

[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 paragraph 16; *Gomboc*, above, at paragraph 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;

ait été abusive (*R. c. Gomboc*, 2010 CSC 55, [2010] 3 R.C.S. 211 (*Gomboc*), au paragraphe 20).

[109] Pour aborder ces questions, les tribunaux doivent adopter « une approche téléologique axée principalement sur la protection de la vie privée considérée comme une condition préalable à la sécurité individuelle, à l'épanouissement personnel et à l'autonomie ainsi qu'au maintien d'une société démocratique prospère » (*R. c. Spencer*, 2014 CSC 43, [2014] 2 R.C.S. 212 (*Spencer*), au paragraphe 15).

a) Qu'est-ce qu'une fouille, une perquisition ou une saisie?

[110] Il y a *saisie* « lorsque les autorités prennent quelque chose appartenant à une personne sans son consentement ». À titre d'exemple, une ordonnance de production de document rendue en vertu d'un règlement constitue une saisie (*Thomson Newspapers Ltd. c. Canada (Directeur des enquêtes et recherches, Commission sur les pratiques restrictives du commerce)*, [1990] 1 R.C.S. 425 (*Thomson Newspapers*), à la page 505 et *R. c. McKinlay Transport Ltd.*, [1990] 1 R.C.S. 627 (*McKinlay*), à la page 642).

[111] En revanche, il y a *fouille* ou *perquisition* lorsqu'une personne visée par une activité envahissante menée par l'État s'attend raisonnablement au respect de sa vie privée quant à l'objet de la fouille ou de la perquisition présumée. Dans l'affirmative, l'activité en question constitue une fouille ou une perquisition pour les fins de l'article 8 (*Spencer*, précité, au paragraphe 16 et *Gomboc*, précité, au paragraphe 20).

[112] L'ensemble des circonstances à évaluer lorsqu'il s'agit de déterminer si la personne visée s'attendait raisonnablement au respect de sa vie privée quant à l'objet de la fouille ou de la perquisition présumée comprend divers facteurs directement liés aux attentes de la personne en matière de respect de la vie privée, d'un point de vue tant subjectif qu'objectif. Il s'agit :

i. de l'objet de la fouille ou de la perquisition présumée;

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 paragraph 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 paragraphs 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. A.M.*, 2008 SCC 19, [2008] 1 S.C.R. 569 (*A.M.*), at paragraph 38).

[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, [2004] 3 S.C.R. 432 (*Tessling*), at paragraph 26). 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 S.C.R. 281 (*Plant*), at page 293 (emphasis added); *Spencer*, above, at paragraph 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 paragraph 32; *Spencer*, above, at paragraph 19; *R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579 (*Patrick*), at paragraph 27).

ii. du droit de la personne à l'égard de l'objet;

iii. de l'attente subjective de la personne en matière de respect de la vie privée relativement à l'objet;

iv. de la question de savoir si cette attente subjective en matière de respect de la vie privée était objectivement raisonnable, eu égard à l'ensemble des circonstances.

(*Spencer*, précité, au paragraphe 18.)

[113] En ce qui a trait au premier des quatre facteurs susmentionnés, il est nécessaire d'évaluer non seulement l'objet de la fouille ou de la perquisition présumée, mais aussi les conclusions qu'il est raisonnable d'en tirer quant aux activités privées ou à d'autres informations privées de la personne (*Spencer*, précité, aux paragraphes 26 à 31). Autrement dit, lorsque des informations sont l'objet d'une fouille ou d'une perquisition, la Cour doit tenir compte de l'importance des informations ainsi obtenues (*R. c. A.M.*, 2008 CSC 19, [2008] 1 R.C.S. 569 (*A.M.*), au paragraphe 38).

[114] La protection garantie par l'article 8 de la Charte ne s'applique pas à tout ce qu'une personne pourrait vouloir garder hors de la portée des agents de l'État (*R. c. Tessling*, 2004 CSC 67, [2004] 3 R.C.S. 432 (*Tessling*), au paragraphe 26). Cette protection se limite plutôt à « un ensemble de renseignements biographiques d'ordre personnel que les particuliers pourraient, dans une société libre et démocratique, vouloir constituer et soustraire à la connaissance de l'État. Il pourrait notamment s'agir de renseignements tendant à révéler des détails intimes sur le mode de vie et les choix personnels de l'individu » (*R. c. Plant*, [1993] 3 R.C.S. 281 (*Plant*), à la page 293 et *Spencer*, précité, au paragraphe 27; non souligné dans l'original).

[115] L'évaluation du deuxième facteur susmentionné (le droit de la personne à l'égard de l'objet de la fouille ou de la perquisition présumée) porte essentiellement sur la mesure dans laquelle ce droit peut être considéré comme direct (*Tessling*, précité, au paragraphe 32; *Spencer*, précité, au paragraphe 19; et *R. c. Patrick*, 2009 CSC 17, [2009] 1 R.C.S. 579 (*Patrick*), au paragraphe 27).

[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 paragraph 19; *Tessling*, above, at paragraph 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 paragraph 37; *Gomboc*, above, at paragraph 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 paragraphs 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 paragraph 50).

[116] L'attente subjective de la personne en matière de respect sa vie privée relativement à l'objet, qui constitue le troisième facteur, peut être établie grâce à des éléments de preuve directs qui la démontrent ou au moyen d'une inférence relative aux circonstances (*Spencer*, précité, au paragraphe 19 et *Tessling*, précité, au paragraphe 38). À titre d'exemple, il existe une présomption relative à l'existence d'une telle attente quant aux activités qui se déroulent dans un domicile (*Patrick*, précité, au paragraphe 37 et *Gomboc*, précité, au paragraphe 25). Toutefois, l'article 8 de la Charte « n'enveloppe pas la maison dans un voile impénétrable de confidentialité » et, lorsqu'aucune fouille ou perquisition n'a été effectuée dans le domicile lui-même, « l'analyse devrait être axée sur le droit au respect du caractère privé des renseignements personnels » (*Gomboc*, précité, aux paragraphes 46 et 49). À cet égard, le fait que la fouille ou la perquisition a pu avoir trait au domicile « doit être considéré comme accessoire par rapport aux renseignements que la technique d'enquête pouvait révéler et a révélés au sujet de la maison » (*Gomboc*, précité, au paragraphe 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 pages 506–507).

[117] En ce qui a trait au quatrième facteur (la question de savoir si l'attente subjective en matière de respect de la vie privée était objectivement raisonnable), « le degré de vie privée auquel le citoyen peut raisonnablement s'attendre peut varier considérablement selon les activités qui le mettent en contact avec l'État » (*Thomson Newspapers*, précité, aux pages 506 et 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;

[118] Pour évaluer ce facteur, il est nécessaire de prendre en considération :

i. la nature du droit au respect de la vie privée qui est en jeu;

ii. les circonstances de la fouille ou de la perquisition présumée;

iii. l'endroit où la fouille ou la perquisition présumée a eu lieu;

iv. la possibilité que les informations aient déjà été abandonnées ou communiquées à des tiers;

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 paragraph 20; *Tessling*, above, at paragraph 32; *Patrick*, above, at paragraph 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 S.C.R. 8 (*Evans*), at paragraph 40; *R. v. Colarusso*, [1994] 1 S.C.R. 20 (*Colarusso*), at page 53). However, it has since stated that it is more logical to consider this factor when considering whether a search was unreasonable (*Tessling*, above, at paragraph 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 paragraph 35; *Tessling*, above, at paragraph 20). The analysis of these categories "turns on the privacy of the area or the 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 paragraph 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

v. les objectifs de l'intrusion;

vi. le degré auquel la technique utilisée pour mener la fouille ou la perquisition a porté atteinte au droit au respect de la vie privée qui est en jeu;

vii. le cadre législatif et contractuel applicable, s'il y a lieu;

viii. la possibilité qu'en soi-même, le recours à la technologie utilisée pour effectuer la fouille, la perquisition ou la surveillance ait été déraisonnable d'un point de vue objectif.

(*Spencer*, précité, au paragraphe 20; *Tessling*, précité, au paragraphe 32; et *Patrick*, précité, au paragraphe 38).

[119] Même si elle a déjà soutenu que la nature de l'objectif de l'État lorsqu'il mène une activité envahissante peut aussi être prise en considération quand il s'agit de déterminer si cette activité constitue une fouille ou une perquisition (*R. c. Evans*, [1996] 1 R.C.S. 8 (*Evans*), au paragraphe 40 et *R. c. Colarusso*, [1994] 1 R.C.S. 20 (*Colarusso*), à la page 53), la Cour suprême a statué depuis qu'il est plus logique de tenir compte de ce facteur lorsqu'il s'agit de déterminer si une fouille ou une perquisition était abusive (*Tessling*, précité, au paragraphe 64, quant à la gravité de l'infraction).

[120] La nature du droit au respect de la vie privée a surtout trait aux lieux, à la personne et aux informations. Ces catégories ne sont pas figées ni mutuellement exclusives (*Spencer*, précité, au paragraphe 35 et *Tessling*, précité, au paragraphe 20). L'analyse de ces catégories «porte sur le caractère privé du lieu ou de l'objet visé par la fouille ou la perquisition ainsi que sur les conséquences de cette dernière pour la personne qui en fait l'objet, et non sur la nature légale ou illégale de la chose recherchée» (*Spencer*, précité, au paragraphe 36).

[121] L'aspect spatial du droit d'une personne au respect de sa vie privée englobe des endroits comme son domicile, sa chambre d'hôtel ou son lieu de travail. L'aspect personnel de ce droit se rapporte à l'intégrité physique de la personne, en particulier son droit de ne

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 paragraphs 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 page 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 paragraph 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 pages 505–508; *Colarusso*, above, at pages 37–38 and 40; *R. v.*

pas se faire toucher ou palper ou de ne pas subir de prélèvements en vue de dévoiler des objets ou des informations qu'elle souhaite dissimuler. L'aspect informationnel de ce droit touche aux informations que la personne souhaite voir demeurer secrètes ou confidentielles, à celles dont elle veut garder le contrôle et à celles qu'elle a communiquées de façon anonyme ou qui concernent des activités qu'elle mène dans l'anonymat (*Spencer*, précité, aux paragraphes 38 à 44).

[122] Au moment de déterminer les paramètres de la protection accordée par l'article 8 de la Charte quant à l'aspect informationnel du droit au respect de la vie privée, il est nécessaire de prendre en considération la nature des informations, le lieu où elles ont été obtenues, la méthode utilisée pour les obtenir ainsi que l'importance de l'objectif de l'État en la matière (*Plant*, précité, à la page 293). Il faut également tenir compte de la possibilité :

i. que l'objet de la fouille ou de la perquisition ait été à la vue du public;

ii. que l'objet de la fouille ou de la perquisition ait été abandonné;

iii. qu'en soi-même, le recours à la technologie utilisée pour effectuer la surveillance ait été déraisonnable d'un point de vue objectif;

iv. que des détails intimes sur le mode de vie de la personne ou des renseignements d'ordre biographique la concernant aient été obtenus.

(*Tessling*, précité, au paragraphe 32.)

[123] En ce qui a trait au cadre législatif et contractuel applicable dont il est question au paragraphe 118 ci-haut, le caractère raisonnable de l'attente d'une personne en matière de vie privée, d'un point de vue objectif, varie en fonction de la nature de ce cadre, par exemple s'il s'agit d'une disposition législative de nature pénale, administrative ou réglementaire ou qui concerne la sécurité nationale. Bref, d'un point de vue objectif, l'attente en matière de vie privée sera bien plus élevée dans un contexte pénal que, bien souvent, dans un contexte

Jarvis, 2002 SCC 73, [2002] 3 S.C.R. 757 (*Jarvis*), at paragraph 62). 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 pages 641–642 and 647–648; *R. v. Wholesale Travel Group Inc*, [1991] 3 S.C.R. 154, at pages 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 pages 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 S.C.R. 145 (*Hunter*), at pages 159–160). 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, [2012] 1 S.C.R. 531 (*Tse*), at paragraph 21).

[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

administratif ou réglementaire (*Thomson Newspapers*, précité, aux pages 505 à 508; *Colarusso*, précité, aux pages 37, 38 et 40; et *R. c Jarvis*, 2002 CSC 73, [2002] 3 R.C.S. 757 (*Jarvis*), au paragraphe 62). Autrement dit, une intrusion étatique peut constituer une fouille, une perquisition ou une saisie dans un contexte pénal, mais ne correspondre à aucune de ces trois réalités dans un autre contexte (*McKinlay*, précité, aux pages 641, 642, 647 et 648 et *R. c. Wholesale Travel Group Inc.*, [1991] 3 R.C.S. 154, aux pages 226 et 227).

[124] Enfin, lorsqu'il existe un cadre législatif et contractuel applicable, il est nécessaire de tenir compte de la nature de la relation entre les parties à ce cadre, de la possibilité que le dépositaire des informations ait été tenu, par contrat, d'en maintenir la confidentialité ainsi que de la possibilité qu'une relation de confiance unisse cette personne et celle dont le droit au respect de la vie privée est en jeu (*Plant*, aux paragraphes 294 à 295).

b) Qu'est-ce qu'une fouille ou une perquisition abusive?

[125] L'article 8 de la Charte ne protège pas contre toute fouille et perquisition, seulement contre celles qui sont abusives.

[126] De façon générale, pour déterminer si une fouille ou une perquisition est abusive, il faut déterminer si, «dans une situation donnée, le droit du public de ne pas être importuné par le gouvernement doit céder le pas au droit du gouvernement de s'immiscer dans la vie privée des particuliers afin de réaliser ses fins» (*Hunter et autres c. Southam Inc.*, [1984] 2 R.C.S. 145 (*Hunter*), aux pages 159 et 160). Pour ce faire, le tribunal doit souvent prendre en compte le droit au respect de la vie privée d'une ou de plusieurs personnes par rapport aux intérêts liés à la sécurité publique, dont le droit à la vie, à la liberté et à la sécurité des personnes qui risquent de subir de graves dommages (*R. c. Tse*, 2012 CSC 16, [2012] 1 R.C.S. 531 (*Tse*), au paragraphe 21).

[127] En bref, l'endroit «où se situe la ligne de démarcation constitutionnelle entre ce qui est abusif et ce qui ne l'est pas […] dépend de l'importance de l'objectif

on the individual's privacy interest" (*R. v. Rodgers*, 2006 SCC 15, [2006] 1 S.C.R. 554 (*Rodgers*), at paragraph 27; *A.M.*, above, at paragraphs 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 paragraph 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 page 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 paragraph 68; *Goodwin v. British Columbia (Superintendent of Motor Vehicles)*, 2015 SCC 46, [2015] 3 S.C.R. 250 (*Goodwin*), at paragraph 56; *Hunter*, above, at pages 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 pages 166–168). In some contexts, including the national security context, this "reasonable grounds to believe" standard may be flexible (*Hunter*, above, at page 168; *Rodgers*, above, at paragraph 35; *R. v. Chehil*, 2013 SCC 49, [2013] 3 S.C.R. 220 (*Chehil*), at paragraph 23). 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

de l'État et de l'incidence de la mesure sur le droit à la vie privée de l'intéressé» (*R. c. Rodgers*, 2006 CSC 15, [2006] 1 R.C.S. 554 (*Rodgers*), au paragraphe 27 et *A.M.*, précité, aux paragraphes 36 et 37).

[128] Partant, «si une personne n'a qu'une attente minimale pour ce qui est des aspects informationnels de sa vie privée, cela pourrait faire pencher la balance en faveur de l'intérêt de l'État» (*Jarvis*, précité, au paragraphe 71).

[129] Quoi qu'il en soit, l'intrusion de l'État dans la vie privée d'une personne ne saurait être justifiée que si elle n'outrepasse pas les besoins de ce dernier quant à l'atteinte de son objectif légitime (*Thomson Newspapers*, précité, à la page 495).

[130] Puisque l'objectif fondamental de l'article 8 est de protéger les personnes contre les intrusions injustifiées de l'État dans leur vie privée, toute autorisation relative à une telle intrusion doit, en principe, être obtenue *au préalable*. Autrement dit, sera présumée abusive une fouille ou une perquisition qui n'a pas été autorisée au préalable par un arbitre tout à fait neutre et impartial qui est en mesure d'exercer des fonctions judiciaires en établissant un équilibre entre les intérêts de l'État et ceux de la personne (*Spencer*, précité, au paragraphe 68; *Goodwin c. Colombie-Britannique (Superintendent of Motor Vehicles)*, 2015 CSC 46, [2015] 3 R.C.S. 250 (*Goodwin*), au paragraphe 56; et *Hunter*, précité, aux pages 160 à 162).

[131] En outre, l'arbitre neutre doit être convaincu que la personne qui demande l'autorisation a des motifs raisonnables de croire, déclarés sous serment, que les conditions applicables qui ont trait à la loi, entre autres, et qui sont préalables à l'exercice du pouvoir de fouille ou de perquisition ont effectivement été réunies (*Hunter*, précité, aux pages 166 à 168). Dans certains contextes, dont celui de la sécurité nationale, le critère des «motifs raisonnables de croire» peut avoir une certaine souplesse (*Hunter*, précité, à la page 168; *Rodgers*, au paragraphe 35 et *R. c. Chehil*, 2013 CSC 49, [2013] 3 R.C.S. 220 (*Chehil*), au paragraphe 23). À titre d'exemple, un degré élevé de fiabilité peut justifier l'imposition d'une norme judiciaire moins rigoureuse, par

paragraph 67). This is particularly so where the intrusion is minimal and narrowly targeted (*A.M.*, above, at paragraphs 13 and 42; *R. v. Kang-Brown*, 2008 SCC 18, [2008] 1 S.C.R. 456 (*Kang-Brown*), at paragraphs 25, 60, 210 and 213; and *Chehil*, above, at paragraph 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, 457 F.T.R. 1 (*Mahjoub*), at paragraph 35).

[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 paragraph 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 paragraph 48; *Wakeling v. United States of America*, 2014 SCC 72, [2014] 3 S.C.R. 549 (*Wakeling*), at paragraph 41; *Rodgers*, above, at paragraph 25; *R. v. Collins*, [1987] 1 S.C.R. 265, at page 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 paragraphs 57 and 71–72; *Thomson Newspapers*, above, at pages 596–597; *Wakeling*, above, at paragraph 77). Depending upon the circumstances and the legislative scheme, the availability of after-the-fact oversight may assist to overcome

exemple « motifs raisonnables de soupçonner », pour octroyer le pouvoir de procéder à une fouille ou à une perquisition (*Goodwin*, précité, au paragraphe 67). Cela est particulièrement vrai lorsque l'intrusion est minimale et très ciblée (*A.M.*, précité, aux paragraphes 13 et 42; *R. c. Kang-Brown*, 2008 CSC 18, [2008] 1 R.C.S. 456 (*Kang-Brown*), aux paragraphes 25, 60, 210 et 213; et *Chehil*, précité, au paragraphe 28). En de telles circonstances, la personne chargée de procéder à la fouille ou à la perquisition après avoir satisfait au critère de soupçons raisonnables n'a pas à demander une autorisation préalable à un arbitre neutre (*Kang-Brown* et *Mahjoub (Re)*, 2013 CF 1096 (*Mahjoub*), au paragraphe 35).

[132] Lorsqu'il y a exigence présumée d'une autorisation préalable, il incombe à la personne qui a procédé à la fouille ou à la perquisition sans mandat de démontrer qu'il n'était pas possible d'obtenir une telle autorisation (*Kang-Brown*, précité, au paragraphe 59).

[133] Par ailleurs, cette personne peut surmonter l'apparence d'illégalité relative aux fouilles et aux perquisitions effectuées sans mandat, c'est-à-dire qu'elle peut démontrer que l'activité était autorisé par la loi, que la disposition législative l'autorisant est raisonnable et que la fouille ou la perquisition n'a pas été effectuée de manière abusive (*Goodwin*, précité, au paragraphe 48; *Wakeling c. États-Unis d'Amérique*, 2014 CSC 72, [2014] 3 R.C.S. 549 (*Wakeling*), au paragraphe 41; *Rodgers*, précité, au paragraphe 25; et *R. c Collins*, [1987] 1 R.C.S. 265, à la page 278).

[134] Pour évaluer le caractère raisonnable d'une disposition législative autorisant la réalisation de fouilles ou de perquisitions sans mandat, il est nécessaire de prendre en considération la nature et l'objet de cette disposition, l'ampleur de l'intrusion qu'elle autorise, le mécanisme d'intrusion qu'elle permet d'utiliser, la supervision judiciaire qu'elle prévoit ainsi que toute autre mesure de responsabilisation ou de contrôle qu'elle comporte pour limiter la portée de l'empiètement de l'État sur le droit d'une personne au respect de sa vie privée (*Goodwin*, précité, aux paragraphes 57, 71 et 72; *Thomson Newspapers*, précité, aux pages 596 et 597; et *Wakeling*, précité, au paragraphe 77). En fonction des circonstances

the presumptive unlawfulness of a warrantless search (*Goodwin*, above, at paragraph 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 paragraph 67, quoting *Chehil*, above, at paragraph 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 (*A.M.*, above, at paragraphs 39–40; *Gomboc*, above, at paragraph 40; *Tessling*, above, at paragraph 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 [***] 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 [***] 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 [***] wireless devices, and thereby enable CSIS to identify those devices and attribute them to him.

[138] According to [***] the individual or individuals who are the subject of a CSS operation ordinarily are known [***] Therefore, it is important to keep in mind

et du régime législatif, la disponibilité d'une surveillance a posteriori peut aider à surmonter l'apparence d'illégalité relative aux fouilles et aux perquisitions effectuées sans mandat (*Goodwin*, précité, au paragraphe 71).

[135] En ce qui a trait à la manière dont s'effectue la fouille ou la perquisition, il est nécessaire d'évaluer la fiabilité ou la précision des mécanismes utilisés et le possible degré d'intrusion dans la vie privée de personnes innocentes. À cet égard, « "[u]ne méthode de fouille qui aurait pour effet de viser un nombre démesuré de personnes innocentes ne saurait être jugée non abusive" » (*Goodwin*, précité, au paragraphe 67, citant *Chehil*, précité, au paragraphe 51).

[136] Quoi qu'il en soit, le tribunal doit évaluer ce que permet de faire à l'heure actuelle la technologie ou le mécanisme utilisé pour procéder à la fouille ou à la perquisition, pas ce qu'il pourrait un jour permettre de faire (*A.M.*, précité, aux paragraphes 39 et 40; *Gomboc*, précité, au paragraphe 40; et *Tessling*, précité, au paragraphe 29).

2) *Application des principes juridiques aux faits en l'espèce*

a) L'utilisation de la technologie relative aux ESB par le SCRS constitue-t-elle une « fouille » ou une « perquisition »?

[137] En l'espèce, le SCRS a utilisé la technologie relative aux ESB dans l'unique objectif d'intercepter les IMSI et les IMEI des appareils mobiles de [***] afin d'être en mesure, par la suite, de reconnaître ces appareils et de les lui attribuer. Le SCRS n'a pas utilisé cette technologie pour géolocaliser [***] La procureure générale reconnaît qu'un mandat serait nécessaire pour en faire une telle utilisation. Partant, l'évaluation ci-dessous portera uniquement sur l'utilisation de la technologie relative aux ESB pour recueillir les IMSI et les IMEI ayant trait aux appareils mobiles de [***] afin de permettre au SCRS de reconnaître ces appareils et de les lui attribuer.

[138] Selon [***] les cibles d'une opération fondée sur des ESB sont habituellement connues [***] Il est donc important de garder à l'esprit qu'en général, le SCRS

that CSIS will ordinarily already know certain things about such individuals at the time the CSS operation is conducted. Those things include their location [***] even though their [***] 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. [***] 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 [***]

possède déjà des informations sur ces personnes à ce moment. Par exemple, il sait où elles se trouvent, [***] même s'il ignore peut-être leurs [***]

[139] Je rappelle au passage qu'à une exception près, les ESB et le matériel connexe qu'utilise actuellement le SCRS ne peuvent pas intercepter le contenu des communications. [***] Selon la preuve au dossier, le SCRS s'est donné comme politique de ne pas recueillir du contenu de ce type. À mon avis, pour ce faire, il lui faudrait un mandat.

[140] Selon la procureure générale, l'article 8 de la Charte ne s'applique pas à l'utilisation de la technologie relative aux ESB par le SCRS pour obtenir l'IMSI et l'IMEI d'un appareil mobile parce qu'en général, les particuliers n'ont pas d'attente raisonnable en matière de vie privée à l'endroit de ces indicateurs. Je ne suis pas d'accord. Selon moi, la prise en considération de l'ensemble des circonstances, tel que discuté ci-dessous, et l'adoption d'une approche téléologique à l'égard de l'article 8 de la Charte donnent à penser que les particuliers ont bel et bien une attente raisonnable en matière de vie privée à l'endroit de ces numéros et des informations qu'ils permettent au SCRS d'obtenir ou d'inférer. Partant, l'utilisation de la technologie relative aux ESB constitue une fouille, ce qui vient répondre au premier des deux critères ayant trait à l'article 8.

i) Objet de l'intrusion

[141] La procureure générale soutient que les IMSI et les IMEI obtenues au moyen de la technologie relative aux ESB ne sont que des numéros anodins qui révèlent simplement l'indicatif de pays de l'abonné, l'identité de son FST et son numéro d'identification unique ainsi que la marque, le modèle et le numéro de série de l'appareil mobile. Elle ajoute que ces informations ne révèlent rien sur les données biographiques ou sur la vie privée de la personne et n'ont pas tendance à révéler des détails intimes sur le mode de vie et les choix personnels de l'individu. À titre d'exemple, en l'espèce, l'opération fondée sur des ESB a [***] révélé [***]

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

[144] Although [***] 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 [***] This may well have been what [***] was referring to when he testified that IMSI and IMEI information is required "in order to be able to determine [***] and communication patterns and a bunch of other additional elements in regards to undergoing national security investigations." [***] 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 and 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 (*Gone Opaque*), at page 15).

[142] Pour appuyer son opinion, selon laquelle l'article 8 de la Charte ne s'applique pas à ces informations, la procureure générale accorde beaucoup de crédit aux arrêts *Tessling*, *Gomboc* et *Plant*, précités, dans lesquels la Cour suprême du Canada a statué que l'article 8 de la Charte ne s'appliquait pas à la collecte d'informations relatives à la quantité de chaleur qui émane d'une maison, à la quantité d'électricité qu'y achemine le réseau ni aux documents portant sur la quantité d'électricité qu'on y consomme, respectivement.

[143] Toutefois, [***] employé de niveau supérieur du SCRS, [***] a affirmé dans un affidavit [TRADUCTION] « [qu']au fil du temps, les IMSI et les IMEI d'une cible peuvent permettre de dégager des habitudes » (non souligné dans l'original). [***]

[144] Même si [***] n'en a pas parlé, l'obtention de l'IMSI ou de l'IMEI d'une cible pourrait fort bien mener au dévoilement d'autres informations, par exemple les habitudes de communications de cette personne [***] Il est possible que ce soit ce dont parlait [***] lorsqu'il a témoigné que l'IMSI et l'IMEI sont nécessaires « pour déterminer les [***] les habitudes de communication et de nombreux autres éléments relatifs à des enquêtes en cours en matière de sécurité nationale ». [***] la collecte de l'IMSI et de l'IMEI se distingue des questions soulevées dans les arrêts *Tessling*, *Gomboc* et *Plant*, précités.

[145] En outre, dans un rapport déposé en l'espèce à titre de pièce nº 16, il est souligné que [TRADUCTION] « l'IMSI et l'IMEI peuvent aussi servir à recenser des activités numériques comme la navigation Web […] sans même qu'il soit nécessaire d'établir une correspondance entre un profil établi et le nom ou l'adresse d'une personne » (Tamir Israel et Christopher Parsons, *Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada* (Y a-t-il perte de transparence? Analyse de la surutilisation hypothétique des intercepteurs d'IMSI au Canada), Ottawa, Telecom Transparency Project, Samuelson-Glushko Canadian Internet Policy et Public Interest Clinic, 2016 (*Gone Opaque*), à la page 15).

[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 paragraph 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

[146] Je souligne également que [***] a noté que [TRADUCTION] « le Service peut, s'il l'estime nécessaire, communiquer l'IMSI ou l'IMEI obtenue au moyen d'un ESB à des services étrangers, comme tout autre type de renseignement qu'il recueille ». Il a ajouté « qu'avant de communiquer ces informations, le Service évaluera les possibilités qui s'offrent à lui pour minimiser les risques de mauvais traitement pour les personnes dont il divulgue l'identité à ces services étrangers ». À cet égard, il a affirmé qu'à sa connaissance, le SCRS avait communiqué à [***] reprises, à des services étrangers, des IMSI et des IMEI recueillies au moyen de la technologie relative aux ESB. Je vais aborder la possible importance de tels échanges d'informations avec des autorités étrangères au paragraphe 168 ci-dessous.

ii) Droit de la personne à l'égard de l'objet

[147] Manifestement, [***] bénéficie d'un droit direct à l'égard des IMSI et des IMEI liées à des appareils mobiles et obtenues par le SCRS dans le cadre de l'opération fondée sur des ESB. Il en serait de même pour les IMSI et les IMEI liées aux appareils mobiles d'autres cibles du SCRS, peu importe si leur identité est connue. La procureure générale n'a pas laissé entendre le contraire.

iii) Les personnes ont-elles une attente subjective en matière de vie privée relativement à l'objet?

[148] Aucun élément de preuve relatif aux attentes subjectives de [***] ou de quiconque à l'égard de l'IMSI et de l'IMEI liées à leurs appareils mobiles n'a été déposé en l'espèce. Cependant, il ne s'agit pas d'un critère très exigeant (*Patrick*, précité, au paragraphe 37). Je conviens avec les *amici* qu'il est possible de présumer qu'en général, les personnes ont vraisemblablement l'attente subjective que toute information relative à leurs appareils mobiles susceptible d'être communiquée aux tours de téléphonie cellulaire relevant de leur FST ne sera pas interceptée subrepticement par des agents de l'État, comme le SCRS, ou par quiconque, au moyen de fausses tours de téléphonie cellulaire. Cela dit, la plupart

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 [***] 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, [***] 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 paragraph 37; *Gomboc*, above, at paragraph 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 [***] (*Spencer*, above, at paragraphs 42–49).

des personnes n'ont vraisemblablement pas conscience que leurs appareils mobiles communiquent aux tours de téléphonie cellulaire des informations susceptibles de révéler des renseignements personnels les concernant que des agents de l'État pourraient intercepter.

iv) Dans l'affirmative, une telle attente est-elle objectivement raisonnable?

Nature du droit au respect de la vie privée en l'espèce

[149] Le droit des personnes à l'égard des renseignements personnels liés à leurs appareils électroniques mobiles et à l'utilisation qu'ils en font constitue les principaux aspects du droit au respect de la vie privée que compromet l'utilisation, par le SCRS, de la technologie relative aux ESB pour intercepter des IMSI et des IMEI, et ce, dès que le Service recueille ces chiffres, puis lorsqu'il les utilise pour établir un profil des [***] et des habitudes de communication de la personne.

[150] Dans la mesure où cette technologie peut révéler des informations sur les personnes avec lesquelles communiquent des cibles lorsqu'elles se trouvent à différents endroits, [***] l'utilisation de cette technologie touche également à l'aspect spatial du droit au respect de la vie privée. En l'espèce, cet aspect est très secondaire par rapport à l'aspect informationnel (*Spencer*, précité, au paragraphe 37 et *Gomboc*, précité, au paragraphe 49). Cela est attribuable au fait qu'en général, le SCRS sait où se trouve sa cible lorsqu'il mène une opération fondée sur des ESB pour recueillir les IMSI et les IMEI des appareils mobiles qu'elle a en sa possession.

[151] L'aspect informationnel du droit au respect de la vie privée regroupe divers éléments compromis par la collecte et l'analyse subséquente de l'IMSI et de l'IMEI par le SCRS : la confidentialité de ces numéros, le contrôle que la cible exerce sur ceux qui y ont accès ainsi que le droit de la personne à l'anonymat quant i) à ses liens avec ses interlocuteurs éventuels et ii) aux lieux où ces communications peuvent être effectuées, [***] (*Spencer*, précité, aux paragraphes 42 à 49).

The Circumstances in which IMSI and IMEI Identifiers Are Obtained

[152] According to [***] 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 [of the Act] [***] 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, [***] 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] [***]

[154] [***]

[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 [***]

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

Circonstances entourant l'obtention de l'IMSI et de l'IMEI

[152] Selon [***] le SCRS utilise la technologie relative aux ESB pour obtenir l'IMSI et l'IMEI en vue d'attribuer un appareil mobile à la cible d'une enquête menée au titre de l'article 12 [***] de la Loi sur le SCRS. Comme il a été mentionné, au moment de l'opération fondée sur des ESB, ces personnes sont généralement des cibles du SCRS. Partant, le SCRS détient différentes informations à leur sujet, notamment où elles se trouvent, [***] le SCRS connaît habituellement l'identité de la cible lorsqu'il lance une opération fondée sur des ESB.

Lieu de la collecte de l'IMSI et de l'IMEI et méthode utilisée

[153] [***]

[154] [***]

[155] Peu importe où se trouve la cible, la collecte, par le SCRS, des IMSI et des IMEI des appareils mobiles de l'individu au moyen de la technologie relative aux ESB ne révèle rien de plus concernant ses appareils mobiles ou ses activités sur les lieux [***]

[156] Comme expliqué aux paragraphes 70 à 73 et 79 ci-haut, selon la preuve produite en l'espèce, les ESB et le matériel connexe qu'utilise le SCRS gardent le contact avec l'appareil mobile d'un individu [***] De plus, le SCRS utilise les ESB d'une manière qui ne nuit d'aucune façon perceptible à la qualité du service dont bénéficient les utilisateurs d'appareils mobiles qui se trouvent à proximité. Également, à une exception près, les ESB et le matériel connexe ne permettent pas d'intercepter le contenu des communications des utilisateurs d'appareils mobiles ni les informations stockées dans ces appareils. L'exception concerne [***] Enfin, le SCRS supprime très rapidement les informations provenant des appareils mobiles de tiers qu'il capture dans le cadre de ses opérations fondées sur des ESB, souvent dans un délai de [***] jours, et certainement dès qu'un rapport opérationnel a été rédigé.

[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, [***]

[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 paragraph 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

[157] Règle générale, les opérations fondées sur des ESB sont menées à l'insu de la cible, bien que celle-ci puisse se douter qu'elle en fait l'objet.

Possibilité que l'ISMI et l'IMEI aient été abandonnées ou divulguées à un ou à plusieurs tiers

[158] La procureure générale accorde une grande importance au fait que les IMSI et les IMEI obtenues dans le cadre d'une opération fondée sur les ESB l'ont été sur les ondes publiques, dans un contexte où ces informations sont « offertes » aux tours de téléphonie cellulaire par l'appareil mobile de la cible. À cet égard, la procureure générale établit un parallèle entre les IMEI et les IMSI communiquées « de plein gré » aux SFT et les informations relatives à la consommation d'électricité fournies aux distributeurs d'électricité dans *Plant*, précité. Elle établit également un parallèle avec des affaires comme *Patrick*, précité, où la Cour a statué qu'une attente raisonnable en matière de vie privée n'existe pas à l'égard d'informations qui ont été « abandonnées » à la poubelle.

[159] Toutefois, selon moi, la moyenne des gens considère probablement que l'IMSI et l'IMEI sont plus confidentielles et personnelles que les données sur sa consommation d'électricité, [***]

[160] De plus, comme dans le cas de la chaleur qui s'échappe de la maison, la moyenne des gens ne croit vraisemblablement pas avoir « abandonné » l'IMSI et l'IMEI lorsque l'appareil mobile communique ces identificateurs aux tours de téléphonie cellulaire (*Tessling*, précité, au paragraphe 41). Comparativement à des informations jetées à la poubelle, qui aboutissent à la décharge publique où elles peuvent être recueillies par des personnes autres que celles qui travaillent à la collecte des ordures et au processus d'élimination, la moyenne des gens croit que l'IMSI et l'IMEI seront conservées en toute confidentialité par le FST, sauf si les services de police obtiennent un mandat afin de les obtenir. Comparativement à la renonciation implicite aux droits en matière de vie privée qui peut être accordée afin de permettre au public de s'approcher d'une demeure à des

the homeowner to be legitimate (*Evans*, above, at paragraphs 6 and 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 [***] CSIS cannot access the content of communications made on the mobile device.

[162] [***] begin to put together an initial profile of the subject of investigation's [***] 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. [***]

[163] Although CSIS may be able to begin putting together an initial profile of the subject of investigation's [***] 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. [***]

The Relevant Statutory and Contractual Framework

[164] The relevant statutory framework within which CSIS conducts CSS operations for the purposes of

fins jugées légitimes par le résidant (*Evans*, précité, aux paragraphes 6 et 14), une telle renonciation n'existe pas à l'endroit du grand public en ce qui a trait à l'IMSI et à l'IMEI lorsque les appareils mobiles communiquent ces informations dans un environnement cellulaire.

Mesure dans laquelle la technique de fouille ou de perquisition est envahissante à l'égard du droit au respect de la vie privée

[161] Selon moi, la technologie relative aux ESB est minimalement envahissante en ce qui a trait aux aspects informationnel et spatial du droit au respect de la vie privée. Au départ, tout ce qui est recueilli est une version « simple » des IMSI et des IMEI qui ne révèle que le FST d'une personne, son numéro MSIN ainsi que la marque, le modèle et le numéro de série de l'appareil mobile. Ni l'appareil mobile ni son contenu n'est consulté d'aucune façon. De la même manière, aucune information pouvant se trouver dans l'appareil n'est recueillie et, sauf pour ce qui est [***] le SCRS ne peut pas avoir accès au contenu des communications effectuées au moyen de l'appareil mobile.

[162] [***] et habitudes de communication de la cible. Il s'agit des informations qui peuvent aider le SCRS à établir « les motifs raisonnables de croire » nécessaires pour obtenir un mandat, tels que l'indiquent les paragraphes 21(1), 21(3), 21(3.1), 21.1(1), 21.1(3) et 21.1(4) de la Loi sur le SCRS, ou faire renouveler un mandat en vertu de l'article 22. [***]

[163] Alors que le SCRS peut commencer à dresser un profil initial des [***] et des habitudes de communication de la cible, il est difficile de voir comment il pourrait en tirer des conclusions qui seraient particulièrement justes ou auraient un caractère envahissant concernant les activités personnelles de cette personne. [***]

Cadre législatif et contractuel applicable

[164] Le mandat accordé au SCRS en vertu de l'article 12 de la Loi sur le SCRS lui sert de cadre législatif

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.

pour mener des opérations fondées sur des ESB afin d'attribuer un appareil sans fil à une cible connue. Conformément à cette disposition, le SCRS recueille, dans une mesure strictement nécessaire, analyse et conserve les informations et les renseignements concernant des activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent une menace envers la sécurité du Canada. Pour les motifs exposés au paragraphe 119, je tiendrai compte des intérêts de l'État en matière de sécurité à la deuxième étape de l'analyse ayant trait à l'article 8 de la Charte, qui est traitée à la partie VII.C.2)b) des présents motifs. Pour le moment, je continuerai de me pencher uniquement sur le point de vue des personnes qui peuvent faire l'objet d'activités envahissantes par le SCRS en vertu de l'article 12 de la Loi sur le SCRS.

[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.

[165] La procureure générale soutient que le contexte de sécurité nationale dans lequel peuvent se dérouler les opérations du SCRS est plus près des contextes réglementaire et administratif que du contexte du droit pénal. Bref, elle semble affirmer que les individus ont des attentes moindres en matière de vie privée dans un contexte de sécurité nationale que dans un contexte pénal, car ce premier contexte n'entraîne pas souvent des poursuites criminelles contre des particuliers et n'entrave donc pas le droit à la liberté. En d'autres mots, il est moins probable qu'une personne soit poursuivie, en totalité ou en partie, à cause de renseignements personnels recueillis par le SCRS qu'à cause de renseignements de même nature obtenus par les services de police.

[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.

[166] Selon moi, à elle seule, cette explication n'est pas suffisante pour conclure qu'un individu a des attentes moindres en matière de vie privée dans le contexte de sécurité nationale que dans le contexte pénal.

[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, [2008] 2 S.C.R. 326 (*Charkaoui II*), at paragraph 53), the nature

[167] Au moment de déterminer si une personne peut avoir une attente raisonnable en matière vie privée relativement aux renseignements personnels recueillis par des agents de l'État, la pertinence du contexte législatif entourant la collecte des informations dépend de la gravité des conséquences potentielles pour cette personne (*Charkaoui c. Canada (Citoyenneté et Immigration)*, 2008 CSC 38, [2008] 2 R.C.S. 326 (*Charkaoui II*), au

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 pages 495–496 and 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 paragraph 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 pages 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

paragraphe 53), de la nature du comportement visé par la loi, et des fins auxquelles la loi a été promulguée pour réglementer le comportement (*Thomson Newspapers*, précité, aux pages 495, 496, 509 et 510).

[168] En ce qui a trait aux conséquences possibles, les activités d'enquête menées par le SCRS en vertu de l'article 12 peuvent très facilement entraîner des conséquences plus graves pour les individus que celles qui se déroulent dans un contexte pénal (*Charkaoui II*, précité, au paragraphe 54). Cela comprend le renvoi vers des pays où les individus peuvent être menacés de mort ou subir des peines d'emprisonnement plus longues qu'au Canada. De plus, les informations recueillies par le SCRS peuvent non seulement être communiquées à des organismes d'application de la loi et d'autres agents d'État au Canada et, en fin de compte, entraîner des accusations criminelles, mais elles peuvent également être communiquées à des gouvernements étrangers. En effet, comme le précise le paragraphe 146 ci-haut, [***] a expressément soulevé cette possibilité en ce qui a trait à l'IMSI et à l'IMEI. Entre autres, cela peut nuire considérablement à une personne qui cherche à se rendre à l'étranger, à obtenir un nouvel emploi ou à conserver son emploi. De plus, faire l'objet d'une enquête en vertu de la Loi sur le SCRS entraîne probablement un préjugé plus proche de celui qui est associé à une déclaration de culpabilité pour un crime grave que de tout préjugé relatif à une déclaration de culpabilité pour une infraction contre le bien-être public ou de nature réglementaire ou économique, même lorsqu'une lourde peine d'emprisonnement a été imposée (*Thomson Newspapers*, précité, aux pages 509 à 517).

[169] En ce qui a trait à la nature du comportement mentionné à l'article 12 de la Loi sur le SCRS, je crois que la plupart des activités correspondant à la définition de « menaces envers la sécurité du Canada » figurant à l'article 2 de la Loi sur le SCRS ressemblent davantage aux « vrais » crimes qui font l'objet des lois pénales qu'aux infractions visées par la législation ayant trait au bien-être public, aux règlements et à l'économie.

[170] Alors que la nature du comportement visé par cette législation est telle qu'il est possible de présumer que les personnes ont accepté certaines conditions au

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 pages 505–506, 508–509 and 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 S.C.R. 406, at pages 443-447; *Colarusso*, above, at pages 37–38 and 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

moment d'intégrer les domaines économique ou réglementaire ou au moment de leur arrivée au pays, je ne crois pas qu'il en va de même, du moins dans une certaine mesure, pour les activités qui peuvent faire l'objet d'une surveillance accrue de la part du SCRS en vertu de l'article 12. Le public s'attend probablement à ce que le SCRS, dont il reconnaît que c'est le rôle, enquête sur les menaces envers la sécurité du Canada. Par contre, il s'attend probablement aussi à ce que ces enquêtes ne puissent être menées que si elles sont assujetties à des mesures visant à protéger ses droits garantis par la Charte ou à imposer des limites raisonnables à toute intrusion les concernant. Cet élément sera évalué à la partie VII.C.2)b) des présents motifs.

[171] En ce qui a trait à l'objet de la loi, de nouveau, je crois que les enquêtes sur les menaces envers la sécurité du Canada effectuées en vertu de l'article 12 et la collecte d'informations ou de renseignements effectuée en vertu de l'article 16 de la Loi sur le SCRS ont plus de points communs avec l'objet des lois pénales qu'avec l'objet sous-jacent de la législation ayant trait au bien-être public, aux règlements et à l'économie, pour laquelle les attentes en matière de vie privée sont faibles (*Thomson Newspapers*, précité, aux pages 505 à 506, 508 à 509 et 515 à 516; *Comité paritaire de l'industrie de la chemise c. Potash; Comité paritaire de l'industrie de la chemise c. Sélection Milton*, [1994] 2 R.C.S. 406, aux pages 443 à 447 et *Colarusso*, précité, aux paragraphes 37, 38 et 40). Par contre, j'admets que le public est probablement prêt à concéder *une partie* de ses droits en matière de vie privée afin de permettre au SCRS d'enquêter sur des activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada. Toutefois, en l'absence d'observations de la procureure générale ou des *amici* concernant la nature de telles concessions, il m'est difficile d'en discuter de façon abstraite. Selon moi, elles feront probablement l'objet de discussions à une date ultérieure et seront évaluées à la lumière de leurs contextes respectifs.

[172] En ce qui a trait à l'IMSI et à l'IMEI, je suis convaincu que les individus dont les activités peuvent faire l'objet d'une enquête en vertu de l'article 12 de la Loi sur le SCRS et dont le droit à l'anonymat peut être

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 "[***] or communications patterns" [***] (ii) drawing inferences about [***] 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 paragraphs 37 and following. In one passage, Justice Noël observed as follows:

> … The ODAC processes and analyzes data such as (but not limited to): [***] 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 [***]
>
> (*X (Re)*, above, at paragraph 42).

compromis par ce que le SCRS est en mesure de faire avec ces informations n'ont probablement pas d'attentes réduites en matière de vie privée, et ce, parce qu'ils croiraient probablement, s'ils étaient pleinement informés, que le SCRS peut commencer à en apprendre davantage sur leurs activités privées au moyen des informations obtenues. Comme je l'ai mentionné, cela peut comprendre la création d'un profil personnel les concernant qui peut permettre de i) déterminer leurs [***] et habitudes de communication » [***] ii) tirer des conclusions quant à [***] Le SCRS dispose d'immenses ressources à ces fins, dont le Centre d'analyse des données opérationnelles (CADO) qui a fait l'objet de discussions dans la décision *X (Re)*, au paragraphe 37 et suivants. Dans un passage, le juge Noël fait les observations suivantes.

> […] Les processus et les analyses de données du CADO portent, entre autres, [***] Le produit final, c'est-à-dire le renseignement, donne un portrait précis et intime de la vie et de l'environnement des personnes sur lesquelles le SCRS enquête. Le programme permet d'établir des liens entre diverses sources et d'énormes quantités de données, ce qu'aucun humain n'arriverait à faire. [***]
>
> (*X (Re)*, précitée, au paragraphe 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.

[173] Je suis d'accord avec les *amici* pour dire que ces empiètements possibles sur le droit à l'anonymat d'une personne peuvent faire une différence entre les attentes de ceux dont les activités peuvent faire l'objet d'une enquête ou d'une collecte d'informations par le SCRS et les attentes raisonnables de tiers dont les IMSI et IMEI ont été obtenues de façon fortuite dans le cadre d'une opération du SCRS, puis détruites avant d'être utilisées plus avant. Comme l'ont remarqué les *amici*, la destruction rapide des IMSI et des IMEI concernant des tiers permet de protéger l'anonymat de ces personnes, dont l'anonymat inhérent à l'utilisation, par des individus, de leur appareil mobile.

[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.

[174] Je signale en passant que la procureure générale n'a indiqué aucune mesure législative de nature réglementaire, économique ou autre qui permet, sans mandat, de recueillir subrepticement des informations autrement inaccessibles concernant les téléphones de personnes sans un mandat.

[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 page 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 paragraphs 41 and 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* [Alta. Reg. 160/2003] enacted pursuant to the *Electric Utilities Act*, S.A. 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 paragraphs 31, 33, 82 and 95).

[177] The *amici* also referred to publicly available information, which I agree can be relevant to an assessment

[175] En ce qui a trait au cadre contractuel applicable, aucun élément de preuve n'a été fourni concernant les obligations contractuelles des FST envers leurs abonnés. Toutefois, je conviens avec les *amici* que, si elle avait conscience que ses appareils mobiles divulguent les IMSI et les IMEI dans l'environnement cellulaire lorsqu'ils sont en mode de veille, la personne moyenne croirait probablement que son FST en est le seul destinataire. Cela s'explique en partie par le fait que les personnes jugent, règle générale, que leur téléphone est privé. Ce point important permet de faire une distinction entre les faits en l'espèce et ceux des arrêts *Plant*, *Tessling* et *Gomboc*, précités.

[176] Plus précisément, entre autres facteurs, la Cour suprême a considéré particulièrement pertinents que les membres du public puissent présenter des demandes à la commission municipale de l'électricité concernant la consommation en électricité à une adresse précise (*Plant*, précité, à la page 294). Dans l'arrêt *Tessling*, un facteur qui semble avoir eu de l'importance était que les services de police avaient obtenu des informations sur le chauffage à partir des murs extérieurs du domicile de l'accusé, et qu'il est évident, même pour « l'observateur le moins attentif », qu'une certaine quantité de chaleur émane d'une maison (*Tessling*, précité, aux paragraphes 41, 46 et 47). Par contre, les IMSI et les IMEI liées à des appareils mobiles sont stockées dans ces appareils et ne sont divulguées que dans un environnement cellulaire et uniquement pour avoir accès au réseau cellulaire du FST. Enfin, dans l'arrêt *Gomboc*, la Cour a accordé une importance considérable au fait que l'alinéa 10(3)f) du *Code of Conduct Regulation* [Alta. Reg. 160/2003] adopté en vertu de la *Electric Utilities Act*, S.A. 2003, ch. E-5.1, permettait la divulgation d'informations sur le client [TRADUCTION] « à un agent de la paix pour les besoins d'une enquête relative à une infraction si la communication ne contrevient pas à une demande expresse du client ». La Cour a estimé que M. Gomboc avait bénéficié d'un « préavis exprès quant à la possibilité d'une telle collaboration », mais n'avait pas demandé la confidentialité des renseignements le concernant (*Gomboc*, précité, aux paragraphes 31, 33, 82 et 95).

[177] Les *amici* ont également mentionné les informations accessibles au public, et je conviens également

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 page 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 [***] the *amici* submitted that the evidence of [***] 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. [***] However, given [***] evidence that [***], I do not consider the inference drawn by the *amici* on this point to be strong.

qu'elles peuvent être pertinentes dans le cadre de l'évaluation du caractère raisonnablement objectif de l'attente subjective qu'a probablement une personne que les agents de l'État n'intercepteront pas les IMSI et les IMEI de ses appareils mobiles. Selon moi, ces informations permettent d'étayer le point de vue selon lequel une personne dispose d'une attente raisonnablement objective au sujet du caractère privé des IMSI et des IMEI liées à son appareil mobile.

[178] Plus particulièrement, les *amici* ont noté que la publication *Gone Opaque* dont il est question au paragraphe 145 ci-haut signale que l'Institut européen des normes de télécommunications a fait de la protection de la confidentialité de l'IMSI l'un des cinq objectifs en matière de sécurité en ce qui a trait aux téléphones du système mondial de communications mobiles (GSM) (*Gone Opaque*, à la page 9). À la même page de *Gone Opaque*, il est question d'attribuer des numéros d'identité temporaire d'abonné mobile afin de protéger davantage la confidentialité des IMSI, bien qu'il ne soit pas clair si l'utilisation de tels numéros se limite à l'Europe ou touche le Canada.

[179] Les *amici* ont également fait référence à la page Wikipedia intitulée « International Mobile Subscriber Identity », qui précise que, pour éviter que les abonnés soient reconnus et suivis clandestinement sur l'interface radio, le numéro IMSI est envoyé aussi rarement que possible. Plutôt, un numéro d'identité temporaire d'abonné mobile est généré de façon aléatoire (Wikipedia, « International mobile subscriber identity », en ligne : 2017, <https ://en.wikipedia.org/wiki/International_mobile_subscriber_identity>).

[180] Bien que rien n'atteste [***] les *amici* ont indiqué que les éléments de preuve présentés par [***] concernant les circonstances dans lesquelles un appareil mobile communique l'IMSI et l'IMEI permettent de croire que ces circonstances ont été calibrées minutieusement afin qu'il soit encore plus difficile d'intercepter ces informations subrepticement. [***] Toutefois, compte tenu des éléments de preuve présentés par [***] selon lesquels [***], je ne crois pas que la conclusion des *amici* quant à ce point soit solide.

[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 paragraphs 161–162:

> When conventional means of investigation do not allow to meaningfully advance an investigation, subsections 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 subsections 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.]
>
> Canada. Parliament. Senate. Report of the Special Committee of the Senate on the Canadian Security Intelligence Service, *Delicate Balance: A Security Intelligence Service in a Democratic Society*. Ottawa: Supply and Services Canada (November 1983) (Chair: P.M Pitfield), at page 12, paragraph 31.)

[181] Quoi qu'il en soit, je suis convaincu que les informations susmentionnées tirées du rapport *Gone Opaque* et de Wikipedia souscrivent, dans une certaine mesure, au point de vue selon lequel l'attente subjective d'une personne en matière de vie privée quant aux IMSI et aux IMEI liées à ses appareils mobiles est objectivement raisonnable.

L'utilisation de la technologie relative aux ESB est-elle objectivement déraisonnable?

[182] Les *amici* soutiennent que les ESB et le matériel connexe sont une technologie invasive dont l'utilisation nécessite l'obtention d'un mandat par le SCRS. À cet effet, les *amici* citent le passage suivant de la décision *X (Re)*, aux paragraphes 161 et 162.

> Lorsque les méthodes traditionnelles ne permettent pas de faire progresser une enquête de façon significative, les paragraphes 21(1), 21(2) et l'alinéa 21(2)b) en particulier (désignés ci-après simplement comme l'article 21) entrent en jeu pour permettre au SCRS de demander la délivrance de mandats à la Cour. La demande doit démontrer qu'il existe des motifs raisonnables de croire que les informations demandées sont, sur le plan factuel, liées à une menace envers la sécurité du Canada, comme il en est fait mention aux paragraphes 21(1) et 12(1), et au sens de l'article 2. L'affidavit à l'appui de la demande de mandat et l'interrogatoire tenu ensuite à l'audience sont déterminants pour le juge qui doit décider s'il convient de décerner le mandat. Comme il est bien souligné dans le Rapport Pitfield, dans la discussion sur cette première fonction, la définition de « menaces envers la sécurité du Canada» prévue à l'article 2 de la Loi constitue :
>
> > [...] la limite fondamentale qu'on impose à la liberté d'action du Service. Elle précise des normes essentielles que le SCRS, son directeur et ses employés doivent respecter dans l'exercice de leurs fonctions et jouera un rôle déterminant dans l'appréciation judiciaire du bien-fondé de telle ou telle technique d'enquête par intrusion. [Non souligné dans l'original.]
>
> (Canada. Parlement. Sénat. Rapport du comité sénatorial spécial du Service canadien du renseignement de sécurité, *Équilibre délicat : Un Service du renseignement de sécurité dans une société démocratique.* Ottawa : Approvisionnements et Services Canada (novembre 1983) (Président : P.M Pitfield), à la page 12, au paragraphe 31.)

> 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 subsection 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 [Report of the Special Committee of the Senate on the Canadian Security Intelligence Service, *Delicate Balance: A Security Intelligence Service in a Democratic Society*. Ottawa: Supply and Services Canada (November 1983) (Chair: P.M Pitfield)] that Justice Noël quoted specifically refer to a particular intrusive technique.

[184] In *Tessling*, above, at paragraph 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 paragraph 54, and *Gomboc*, above, at paragraph 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

> L'article 21 s'applique lorsque les méthodes traditionnelles sont insuffisantes pour faire progresser une enquête et qu'il est nécessaire de recourir à des méthodes intrusives. Dans un tel cas, la Cour s'assure que la demande de mandats respecte toutes les exigences de la loi et que les mesures demandées sont justifiées au vu des faits présentés. L'article 21 ne crée pas un régime distinct n'ayant absolument aucun lien avec la première fonction du SCRS comme il est décrit au paragraphe 12(1). Au contraire, l'article 21 vient compléter la première fonction, c'est-à-dire « faire enquête », en établissant des exigences procédurales applicables aux demandes de mandats. [Souligné dans l'original.]

[183] À mon avis, ce passage ne laisse pas entendre que le SCRS doit toujours obtenir un mandat lorsqu'il désire recueillir des informations au moyen d'une nouvelle technologie. En effet, les mots soulignés dans ce passage du Rapport Pitfield [Rapport du comité sénatorial spécial du Service canadien du renseignement de sécurité, *Équilibre délicat : Un Service du renseignement de sécurité dans une société démocratique.* Ottawa : Approvisionnements et Services Canada (novembre 1983) (Président : P. M Pitfield)] que cite le juge Noël s'appliquent à une technique envahissante en particulier.

[184] Dans l'arrêt *Tessling*, précité, au paragraphe 30, la Cour suprême du Canada a clairement indiqué qu'il n'y a pas « d'interdiction distincte visant l'utilisation sans mandat de techniques, électroniques ou autres. » (Voir également *Kang-Brown*, précité, au paragraphe 54 et *Gomboc*, précité, au paragraphe 40.) La question à poser est plutôt : est-ce que la technologie, en fait, « constitue une intrusion dans la sphère raisonnable de vie privée des personnes surveillées? » La réponse à cette question nécessite une évaluation de l'ensemble des circonstances pertinentes. En l'espèce, dans le cadre de cette évaluation, je ne crois pas qu'il ait quoique ce soit relié à l'utilisation de la technologie relative aux ESB en soit qui permette de conclure que cette utilisation est objectivement déraisonnable.

Conclusion concernant le caractère raisonnable des attentes subjectives d'une personne en matière de vie privée à l'égard des IMSI et des IMEI liées à ses appareils mobiles

[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 [***] and communications patterns", [***] (ii) drawing inferences about an individual [***] 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

[185] Selon moi, l'examen téléologique des facteurs qui précèdent permet de conclure au caractère objectivement raisonnable des attentes subjectives d'une personne en matière de vie privée quant aux IMSI et aux IMEI liées à ses appareils mobiles.

[186] Voici les principaux facteurs qui étayent cette conclusion.

i. Les informations concernant les appareils de télécommunication mobiles et leur utilisation sont habituellement considérées comme très personnelles et de nature privée. Cela comprend les informations que le SCRS peut facilement déceler dans le cadre d'une analyse des IMSI et des IMEI, qui peuvent l'aider à créer un profil de la personne en question i) en déterminant ses [***] et ses habitudes de communication, [***] ii) en tirant des conclusions sur [***] Même si le SCRS ne connaît pas l'identité de la personne dont il a recueilli l'IMSI et l'IMEI au moyen de la technologie relative aux ESB, il ne s'agit pas là d'un empiètement négligeable sur le droit d'une personne à l'anonymat. Au sein d'une société démocratique prospère, il est objectivement raisonnable que les individus s'attendent à ce que leurs renseignements personnels demeurent privés et qu'ils ne soient pas recueillis subrepticement par l'État.

ii. Une personne qui fait l'objet d'une enquête ou d'une collecte d'informations en vertu de la Loi sur le SCRS peut subir des conséquences qui peuvent être graves.

iii. Le comportement décrit à l'article 12 de la Loi sur le SCRS ressemble souvent davantage à un « véritable » crime que le type d'infraction visée par la législation relative au bien-être public, aux règlements ou à l'économie dont tient compte la jurisprudence ayant trait à l'article 8 de la Charte.

iv. Le fait que si elle avait conscience que ses appareils mobiles divulguent les IMSI et les IMEI dans l'environnement cellulaire lorsqu'ils sont en

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,

mode de veille, la personne moyenne croirait probablement que son FST en est le seul destinataire.

v. Les informations figurant dans le rapport *Gone Opaque* et sur Wikipedia donnent à penser que certaines mesures ont été adoptées, du moins dans certains domaines de l'industrie des télécommunications, pour protéger la confidentialité des IMSI.

v) Conclusion sur la nature de la collecte de l'IMSI et de l'IMEI : s'agit-il d'une « fouille »?

[187] Compte tenu de ce qui précède, je conclus que la collecte, par le SCRS, des IMSI et des IMEI liées aux appareils mobiles de [***] au moyen la technologie relative aux ESB constitue une « fouille » au sens de l'article 8 de la Charte. Selon moi, cette conclusion est étayée par la nature confidentielle de l'IMSI et de l'IMEI, par la nature personnelle et privée des informations que le SCRS peut être en mesure de rassembler après avoir obtenu ces identificateurs, par la nature directe du droit de [***] à l'égard de ces informations, par l'attente subjective en matière de vie privée qu'a probablement [***] quant à ces informations ainsi que par le caractère raisonnablement objectif de cette attente subjective.

[188] Il convient de souligner que, dans une démocratie prospère, il est objectivement raisonnable que les personnes s'attendent à ce que les renseignements personnels que le SCRS peut obtenir lorsqu'il entreprend d'analyser les IMSI et les IMEI recueillies demeurent privés et qu'ils ne seront pas communiqués à des agents de l'État.

[189] Alors que les atteintes au droit à l'anonymat d'une personne n'ont pas toujours trait à l'article 8 de la Charte, je crois que c'est le cas de la collecte de l'IMSI et de l'IMEI, et ce, en raison des profils que le SCRS peut commencer à esquisser en se fondant sur ces informations. Entre autres, ces profils personnels et techniques peuvent aider le SCRS à assembler une mosaïque qui peut révéler les relations d'une personne

[***] 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 [***] 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 [***] mobile devices constituted a search, and given that CSIS's searches were conducted without a warrant, they were presumptively unreasonable (*Spencer*, above, at paragraph 68; *Goodwin*, above, at paragraph 56; *Hunter*, above, at pages 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 [***] 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

avec une autre, [***] faire des déductions quant aux croyances de la personne. Comme je l'ai déjà indiqué, ce sont ces profils qui peuvent, en fin de compte, aider le SCRS à obtenir un mandat pour obtenir des informations sur l'abonné et entreprendre des activités encore plus envahissantes. Toutefois, jusqu'à ce que le SCRS soit en mesure d'obtenir des informations sur l'abonné et d'exercer d'autres pouvoirs conférés par un mandat, la collecte de l'IMSI et de l'IMEI n'est que minimalement envahissante, et ce, parce que les opérations fondées sur des ESB ne permettent pas au SCRS d'avoir accès à l'appareil mobile, à son contenu, ou à ce qu'il permet de consulter. De plus, sauf pour [***] le SCRS ne peut pas avoir accès au contenu des communications effectuées à l'aide d'appareils mobiles. En outre, il a assuré la Cour qu'il n'utilise pas ses ESB ni le matériel connexe pour avoir accès à un tel contenu.

b) La collecte de l'IMSI et de l'IMEI par le SCRS est-elle abusive?

[190] Puisque la collecte d'IMSI et d'IMEI liées aux appareils mobiles de [***] par le SCRS constitue une fouille, et puisque le Service a procédé à ces fouilles sans mandat, celles-ci sont présumées abusives (*Spencer*, précité, au paragraphe 68; *Goodwin*, précité, au paragraphe 56; et *Hunter*, précité, aux pages 160 à 162).

[191] Pour réfuter cette présomption, et en l'absence de toute suggestion qu'il n'était pas possible d'obtenir un mandat avant que le SCRS n'utilise la technologie relative aux ESB pour recueillir les IMSI et les IMEI liées aux appareils mobiles de [***] la procureure générale doit démontrer que les fouilles étaient autorisées par la loi, que la disposition législative les autorisant est raisonnable et qu'elles n'ont pas été effectuées de manière abusive (voir la jurisprudence citée au paragraphe 133 ci-haut). Ces questions seront traitées ci-dessous.

i) **La fouille était-elle autorisée par la loi?**

[192] La procureure générale soutient que l'utilisation, par le SCRS, de la technologie relative aux ESB pour recueillir des IMSI et des IMEI sans mandat en vue de reconnaître les appareils mobiles d'une cible est autorisée

authorized by section 12 of the Act. As has been noted, that provision states as follows:

Canadian Security Intelligence Service Act, R.S.C., 1985, c. C-23

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.

[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, [2005] 2 S.C.R. 602, at paragraph 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.

par l'article 12 de la Loi sur le SCRS. Comme il en a été question plus haut, cette disposition précise ceci.

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

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.

[193] Les *amici* ne sont pas d'accord avec cette affirmation pour plusieurs raisons, et je traiterai de certaines d'entre elles dans la prochaine section, lorsque j'aborderai la possibilité que le régime établi par les articles 12 et 21 de la Loi sur le SCRS puisse être considéré comme une « disposition législative raisonnable » aux présentes fins.

[194] Selon les *amici*, l'article 12 ne constitue pas un pouvoir distinct d'effectuer une fouille une fois l'article 8 de la Charte invoqué. Ils affirment que cela ne correspondrait pas au libellé des articles 12 et 21, alors qu'« il faut lire les termes d'une loi dans leur contexte global en suivant le sens ordinaire et grammatical qui s'harmonise avec l'esprit de la loi, l'objet de la loi et l'intention du législateur » (*Hypothèques Trustco Canada c. Canada*, 2005 CSC 54, [2005] 2 R.C.S. 602, au paragraphe 10). Plus précisément, ils affirment que l'article 12 précise simplement les fonctions du SCRS et ne l'autorise pas à effectuer des fouilles qui entraînent l'application de l'article 8 de la Charte. À cet effet, ils font une analogie avec le contexte policier, où les services policiers ont le devoir d'enquêter sur les crimes, mais n'ont pas de pouvoir absolu pour effectuer des fouilles. Les *amici* soutiennent que le pouvoir de procéder à une fouille doit être conféré par une loi ou la common law. Toutefois, cela soulève la question de savoir si l'article 12 confère un tel pouvoir.

[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, subsections 21(1), 21(2), and specifically paragraph 21(2)b) … come into play to allow the CSIS to apply for warrants before the Court" (*X (Re)*, above, at paragraph 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 paragraph 30; and in *Kang-Brown*, above, at paragraph 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 analyze 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 paragraphs 21(2)(a) and (b) (*Mahjoub v. Canada (Citizenship and Immigration)*, 2017 FCA 157, 387 C.R.R. (2d) 1 (*Mahjoub FCA*), at paragraph 178). 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

[195] Les *amici* affirment qu'interpréter l'article 12 de la *Loi sur le SCRS* comme une autorisation, pour le personnel du SCRS, d'effectuer des fouilles lorsque l'article 8 de la Charte a été invoqué ne correspond pas à l'interprétation qu'a faite la Cour de cet article. À cet égard, ils soulignent que, dans la décision *X (Re)*, le juge Noël a fait remarquer que « [l]orsque les méthodes traditionnelles ne permettent pas de faire progresser une enquête de façon significative, les paragraphes 21(1), 21(2) et l'alinéa 21(2)b) […] entrent en jeu pour permettre au SCRS de demander la délivrance de mandats à la Cour » (*X (Re)*, précitée, au paragraphe 161). Comme il en est question aux paragraphes 181 et 183 ci-haut, je ne crois pas que le juge Noël, en utilisant l'expression « méthodes traditionnelles d'enquête », veut dire que le SCRS doit obtenir un mandat chaque fois qu'il a recours à une nouvelle technologie ne pouvant pas être qualifiée de « traditionnelle ». Cela irait à l'encontre des enseignements exprès de la Cour suprême dans l'arrêt *Tessling*, précité, au paragraphe 30 et dans l'arrêt *Kang-Brown*, précité, au paragraphe 54.

[196] Selon le libellé simple de l'article 12, le SCRS recueille, au moyen d'une enquête ou autrement, dans la mesure strictement nécessaire, et analyse et conserve les informations et les renseignements sur les activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada. Cela donne au SCRS le pouvoir explicite d'enquêter sur de telles menaces dans ces circonstances.

[197] Les dispositions de l'article 21, qui est lié aux articles 12 et 16, décrivent simplement les circonstances dans lesquelles un mandat peut être demandé et décerné, soit, i) lorsque le directeur du SCRS ou un employé désigné par le ministre à cette fin a des motifs raisonnables de croire que le mandat est nécessaire pour permettre au SCRS d'enquêter sur une menace envers la sécurité du Canada ou d'exercer les fonctions décrites à l'article 16 de la Loi sur le SCRS, et ii) lorsqu'un juge de la Cour est convaincu de ce fait et de ceux qui sont visés aux alinéas 21(2)a) et b) (*Mahjoub c. Canada (Citoyenneté et Immigration)*, 2017 CAF 157 (*Mahjoub CAF*), au paragraphe 178). Il est sous-entendu qu'une telle décision de la part du directeur du SCRS ou de l'employé désigné par le ministre et qu'une telle détermination par la Cour

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

reposent sur les exigences de la common law en ce qui a trait au moment où des mandats sont requis à ces fins.

[198] Selon moi, ni le libellé de l'article 21 ni les autres dispositions de la Loi sur le SCRS n'appuient le point de vue selon lequel le SCRS doit obtenir un mandat chaque fois qu'il effectue une fouille ou une perquisition, au sens de la Charte, qui est minimalement envahissante. Le libellé de l'article 12, conformément à ce qui est établi aux paragraphes 212 à 216 des présents motifs, confère au SCRS toute la latitude nécessaire pour enquêter sans mandat sur des activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada, sauf si la common law l'exige.

[199] Considérer que le SCRS doit obtenir un mandat chaque fois que les attentes raisonnables d'une personne en matière de vie privée sont en jeu confondrait les deux éléments de l'article 8 de la Charte en un seul, c'est-à-dire que cela rendrait inopérante l'exigence voulant qu'une fouille doit être abusive pour enfreindre l'article 8.

[200] Les *amici* suggèrent en outre que le fait d'exiger un mandat avant de tenter d'obtenir des IMSI et des IMEI au moyen de la technologie relative aux ESB correspondrait à l'exigence implicite selon laquelle les services de police doivent obtenir un mandat général, en vertu de l'article 487.01 du *Code criminel*, ou un mandat pour un enregistreur de données de transmission, en vertu de l'article 492.2, avant de pouvoir utiliser un ESB pour obtenir des IMSI et des IMEI et les attribuer à un suspect. Toutefois, le fait que le Parlement *peut* avoir déterminé que les *services de police* doivent avoir un mandat pour utiliser un ESB et attribuer une IMSI et une IMEI à une personne ne suffit pas à conclure que le SCRS doit également obtenir un mandat dans de telles circonstances. Entre autres, les services de police ne disposent pas des pouvoirs conférés par l'article 12 de la Loi sur le SCRS.

[201] Les *amici* soutiennent également qu'il incombe au Parlement de décider de permettre au SCRS d'utiliser un ESB pour intercepter l'IMSI et l'IMEI d'un appareil mobile pour attribuer celui-ci à une cible selon des

"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 analyze 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

«motifs raisonnables de soupçonner». Je suis d'accord, et je crois que c'est ce qu'a fait le Parlement lorsqu'il a adopté l'article 12 de la Loi sur le SCRS. Donc, l'utilisation, par le SCRS, d'un ESB à cette fin précise est «autorisée par la loi», conformément à la jurisprudence citée au paragraphe 133 des présents motifs.

ii) L'article 12 de la Loi sur le SCRS est-il une disposition législative raisonnable?

[202] Comme il en a été question au paragraphe 134 ci-haut, les facteurs dont il faut tenir compte pour évaluer le caractère raisonnable d'une disposition législative autorisant une fouille comprennent la nature et l'objet de cette disposition, l'ampleur de l'intrusion qu'elle autorise, le mécanisme d'intrusion qu'elle permet d'utiliser, la supervision judiciaire qu'elle prévoit ainsi que toute autre mesure de responsabilisation ou de contrôle qu'elle comporte pour limiter la portée de l'empiètement de l'État sur le droit des particuliers au respect de leur vie privée. Selon les circonstances et le régime législatif, la présence d'une supervision peut permettre de surmonter l'apparence d'illégalité relative à une fouille sans mandat. Ces facteurs seront abordés plus loin.

La nature et l'objet de l'article 12

[203] L'article 12 confère au SCRS un rôle central et, sans doute, essentiel, au sein de l'appareil de sécurité nationale du Canada. Il le fait en *exigeant* du SCRS qu'il recueille, au moyen d'enquêtes ou autrement, dans la mesure strictement nécessaire, et analyse et conserve les informations et les renseignements sur les activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada, qu'il en fasse rapport au gouvernement du Canada et qu'il le conseille à cet égard.

[204] Les *amici* affirment que le critère des «motifs raisonnables de soupçonner» prévu à l'article 12 ne suffit pas à justifier que le SCRS effectue une fouille sans mandat. Je ne suis pas d'accord.

[205] Dans le cadre de son analyse de l'article 8 de la Charte, la Cour suprême a rapidement reconnu explicitement que le critère des «motifs raisonnables de croire»

not be required "where state security is involved" (*Hunter*, above, at pages 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 paragraph 23). In brief, the standard required to withstand scrutiny under section 8 "may vary depending on the context" (*Rodgers*, above, at paragraph 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 paragraph 67), particularly where the search is minimally intrusive and narrowly targeted (*A.M.*, above, at paragraphs 13 and 42; *Kang-Brown*, above, at paragraphs 25, 60, 210 and 213).

[208] In each of *Chehil*, *A.M.* 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 S.C.R. 495 (*Simmons*), at pages 527–529; *R. v. Monney*, [1999] 1 S.C.R. 652, at paragraphs 37 and 48) and a search for drugs on a student in a high school by a vice-principal (*R. v. M. (M.R.)*, [1998] 3 S.C.R. 393, at paragraph 50).

[209] Applying the foregoing to CSIS's use of CSS technology to intercept the IMSI and IMEI identifiers of [***] 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

pouvait ne pas être requis lorsqu'il était question de sécurité nationale (*Hunter*, précité, à la page 168).

[206] La Cour a alors réitéré qu'un « exercice de pondération des intérêts en jeu peut justifier une fouille en application d'une norme moins rigoureuse lorsque les droits à la vie privée sont réduits ou lorsque les objectifs d'ordre public de l'État sont prédominants » (*Chehil*, précité, au paragraphe 23). Bref, le critère requis pour résister à un examen approfondi en vertu de l'article 8 peut varier selon le contexte (*Rodgers*, précité, au paragraphe 35).

[207] En plus des circonstances dans lesquelles les droits au respect de la vie privée sont réduits ou les objectifs d'importance publique sont prédominants, la Cour suprême a reconnu qu'un critère plus faible que des « motifs raisonnables de croire » peut être justifié lorsque la méthode utilisée est très précise (*Goodwin*, précité, au paragraphe 67), surtout si la fouille ou la perquisition est minimalement envahissante et étroitement ciblée (*A.M.*, précité, aux paragraphes 13 et 42 et *Kang-Brown*, précité, aux paragraphes 25, 60, 210 et 213).

[208] Dans les arrêts *Chehil*, *A.M.* et *Kang-Brown*, précités, la Cour suprême a conclu que le critère des « motifs raisonnables de soupçonner » ne contrevient pas à l'article 8, malgré l'absence d'une autorisation judiciaire préalable. La Cour en est arrivée à des conclusions semblables en ce qui a trait aux fouilles aux douanes (*R. c. Simmons*, [1988] 2 R.C.S. 495 (*Simmons*), aux pages 527 à 529 et *R. c. Monney*, [1999] 1 R.C.S. 652, aux paragraphes 37 et 48) et à une fouille visant à trouver des stupéfiants sur un élève de niveau secondaire effectuée par un directeur adjoint (*R. c. M. (M.R.)*, [1998] 3 R.C.S. 393, au paragraphe 50).

[209] Chacun des facteurs susmentionnés est présent en ce qui a trait à l'utilisation, par le SCRS, de la technologie relative aux ESB pour intercepter les IMSI et les IMEI des appareils électroniques mobiles de [***] En effet, les objectifs de l'État (c.-à-d. la sécurité nationale) sont prédominants, la fouille est minimalement envahissante, et la méthode utilisée est très précise et étroitement ciblée, puisque les IMSI et les IMEI de tiers

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 [***] 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 paragraphs 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 paragraph 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 S.C.R. 350, at paragraph 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 paragraph 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, analyze 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

n'ont pas été utilisées pour quelque fin que ce soit et ont été détruites rapidement.

[210] Partant, le fait que l'article 12 ait autorisé le SCRS à effectuer une fouille minimalement envahissante des appareils mobiles de [***] parce qu'il avait des « motifs raisonnables de soupçonner » et sans obtenir d'autorisation judiciaire au préalable, ne rend pas, en soi, l'article 12 déraisonnable ou la fouille abusive (*Mahjoub CAF*, précité, aux paragraphes 176 et 177).

[211] En effet, je crois que les objectifs relatifs à la sécurité nationale qui figurent à l'article 12 suffiront habituellement à faire pencher la balance en faveur des intérêts de l'État, lorsque les fouilles menées par le SCRS sont minimalement envahissantes (*Jarvis*, précité, au paragraphe 71 et *Mahjoub CAF*, précité). Comme la Cour suprême l'a reconnu, « [l]'une des responsabilités les plus fondamentales d'un gouvernement est d'assurer la sécurité de ses citoyens ». Il suffit de penser aux récentes attaques terroristes à Barcelone, à Londres, à Paris ou à Berlin, et à l'attaque perpétrée en octobre 2014 contre notre propre parlement, pour prendre conscience des raisons pour lesquelles les intérêts de l'État prédominent généralement lorsque ces intérêts en matière de sécurité nationale entrent en conflit avec le désir d'une personne de ne pas faire l'objet d'une fouille minimalement envahissante. Dans de telles circonstances, le droit à la vie, à la liberté et à la sécurité des personnes qui peuvent subir des dommages sérieux (*Tse*, précité, au paragraphe 21), soit les victimes innocentes d'un attentat terroriste, l'emporte habituellement sur les intérêts en jeu lorsque le SCRS effectue une fouille minimalement envahissante.

[212] Lors de l'évaluation du caractère raisonnable de l'article 12, il est en outre important d'établir si celui-ci a une portée excessive ou s'il est vague. La procureure générale soutient que ce n'est pas le cas de l'article 12, car il impose des critères objectifs et des limites strictes à la collecte d'informations par le SCRS. Je suis d'accord.

[213] Plus particulièrement, le SCRS peut recueillir, analyser et conserver des informations à des fins d'enquête, uniquement sur des activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent

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 paragraphs 3 and 26–37; *Kang-Brown*, above, at paragraph 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 paragraph 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 paragraph 35; affd *Mahjoub FCA*, above, at paragraphs 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 S.C.R. 606, at page 643; *Wakeling*, above, at paragraph 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.

des « menaces envers la sécurité du Canada ». Ce concept est défini précisément à l'article 2 de la Loi sur le SCRS, alors que l'exigence des « motifs raisonnables de soupçonner » est un critère « solide » qui est bien connu en droit canadien (*Chehil*, précité, aux paragraphes 3, 26 à 37 et *Kang-Brown*, précité, au paragraphe 75). Ces paramètres objectifs sont davantage renforcés et restreints par le fait que la portée des informations qui peuvent être recueillies par le SCRS est explicitement limitée à ce qui « est strictement nécessaire ».

[214] Dans la décision *X (Re)*, précitée, au paragraphe 185, le juge Noël a conclu que cette limite s'applique également de façon implicite à la conservation des informations recueillies par le SCRS. Je crois qu'il est important, par courtoisie judiciaire, d'adopter sans autre analyse la position du juge Noël sur le sujet, puisque la Cour se doit de prendre une position cohérente quant à cet enjeu très important. Je prendrai simplement le temps de souligner qu'en l'espèce, ni la procureure générale ni les *amici* n'ont contesté cette interprétation de l'article 12.

[215] Ensemble, ces limites permettent de s'assurer que l'article 12 n'a pas une portée ni excessive, ni trop vague et que les informations recueillies par le SCRS ont un lien rationnel avec l'exécution du mandat conféré au Service par l'article 12. Ces limites assurent également que l'article 12 « atteint le juste équilibre entre l'intérêt du public à ce que l'on fasse enquête sur les menaces envers la sécurité du Canada et les droits à la vie privée de la cible en question » (*Mahjoub*, précité, au paragraphe 35, conf. par *Mahjoub CAF*, aux paragraphes 176 et 177).

[216] Compte tenu de ces limites facilement vérifiables et compréhensibles, on ne saurait affirmer que l'article 12 « manque de précision au point de ne pas constituer un guide suffisant pour un débat judiciaire » (*R. c. Nova Scotia Pharmaceutical Society*, [1992] 2 R.C.S. 606, à la page 643 et *Wakeling*, précité, au paragraphe 62). Au contraire, l'article 12, examiné en corrélation avec la définition de « menaces envers la sécurité du Canada » figurant à l'article 2 de la Loi sur le SCRS, formule clairement la portée des activités qui peuvent faire l'objet d'une enquête par le SCRS.

[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, analyze 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

[217] Compte tenu de ce qui précède, je crois que la nature et l'objet de l'article 12 soutiennent l'opinion selon laquelle il s'agit d'une disposition législative raisonnable.

Degré d'intrusion autorisé par l'article 12

[218] Les limites susmentionnées permettent de s'assurer que le SCRS n'a pas pour mandat d'effectuer des enquêtes envahissantes sur des personnes dont les activités se déroulent à l'extérieur de ces limites. En d'autres termes, l'article 12 n'autorise pas le SCRS à enquêter sur des personnes qui mènent des activités dont il n'existe pas de motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada. Les pouvoirs d'enquête prévus à l'article 12 visent uniquement les personnes dont les activités respectent ce critère rigoureux. En outre, ils ne concernent que la collecte d'informations dans la mesure « strictement nécessaire » ayant trait aux quatre catégories d'activités comprises dans la définition de « menaces envers la sécurité du Canada » figurant à l'article 2 de la Loi sur le SCRS.

[219] Le SCRS peut recueillir, analyser et conserver des informations obtenues de façon non envahissante ou très envahissante au sujet des quelques activités qui s'inscrivent dans le cadre très étroit qu'établit l'article 12. Toutefois, lorsqu'il passe à des activités de collecte plus envahissantes, le Service doit obtenir un mandat. En bref, en ajoutant les dispositions de l'article 21 concernant les mandats à la Loi sur le SCRS, le législateur prévoyait implicitement que le SCRS ne mènerait pas, en vertu de l'article 12, d'activités de collecte plus que minimalement envahissantes sans obtenir une autorisation judiciaire préalable au titre de l'article 21. Il peut être inféré de ce cadre qu'en l'absence d'un mandat, l'article 12 permet au SCRS de mener uniquement des activités non envahissantes ou minimalement envahissantes.

Mesure dans laquelle la Loi sur le SCRS prévoit une supervision judiciaire

[220] Les *amici* soutiennent que l'article 12 n'est pas une disposition législative raisonnable, car il ne fait pas partie des quelques exceptions apportées à l'exigence

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 S.C.R. 223, at page 243), the customs context (e.g., *Simmons*, above, at page 528), "sniffer dog" searches (e.g., *Kang-Brown*, above, at paragraph 60) and searches incident to detention and arrest (e.g., *R. v. Mann*, 2004 SCC 52, [2004] 3 S.C.R. 59, at paragraphs 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 paragraph 24; *A.M.*, above, at paragraph 37; *Rodgers*, above,

d'ordre général selon laquelle les fouilles ou les perquisitions effectuées par des agents de l'État doivent faire l'objet, au préalable, d'une autorisation judiciaire selon le critère des « motifs raisonnables de croire ». À cet égard, ils affirment que les exceptions à l'exigence d'une autorisation judiciaire préalable ne sont reconnues que dans des situations d'urgence (p. ex. *R. c. Grant*, [1993] 3 R.C.S. 223, à la page 243), dans le contexte des douanes (p. ex. *Simmons*, précité, à la page 528), pour les fouilles avec des « chiens renifleurs » (p. ex. *Kang-Brown*, précité, au paragraphe 60) et pour les fouilles accessoires à une détention et à une arrestation (p. ex. *R. c. Mann*, 2004 CSC 52, [2004] 3 R.C.S. 59, aux paragraphes 38 à 40).

[221] Les *amici* soutiennent que dans chacune de ces affaires, la présence d'un contrôle judiciaire a posteriori était un facteur important en l'absence d'une autorisation judiciaire préalable de la fouille. Ils ajoutent qu'aucune méthode de contrôle judiciaire a posteriori n'existe pour les fouilles effectuées sans ou avec mandat en vertu de l'article 21 de la Loi sur le SCRS, car il est possible que la cible n'apprenne jamais qu'elle en a fait l'objet.

[222] Selon moi, les enseignements de la Cour suprême au sujet de la supervision judiciaire d'une fouille (sans mandat) sont plus nuancés que ne le suggèrent les *amici*.

[223] La jurisprudence sur laquelle s'appuient les *amici* n'étaye pas la proposition selon laquelle une fouille minimalement envahissante contrevient nécessairement à l'article 8 de la Charte en l'absence d'une autorisation judiciaire préalable ou d'un contrôle judiciaire a posteriori. Puisque j'ai déjà abordé l'absence d'une autorisation judiciaire préalable aux paragraphes 207 à 210 ci-haut, je limiterai la discussion au contrôle judiciaire a posteriori.

[224] La Cour suprême a toujours maintenu que l'évaluation d'une fouille ou d'une perquisition sans mandat au regard de l'article 8 se fait au cas par cas, selon un juste équilibre entre les intérêts légitimes de l'État et les droits légitimes au respect de la vie privée de la personne qui en fait l'objet (*Kang-Brown*, précité, au paragraphe 24; *A.M.*, précité, au paragraphe 37; *Rodgers*,

at paragraphs 26–27; *Jarvis*, above, at paragraphs 61–62; *Colarusso*, above, at pages 52–53; *McKinlay*, above, at pages 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*, *A.M.* 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 paragraphs 25 and 48–54; *A.M.*, above, at paragraphs 84–86 and 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 paragraph 58), and in part because "[t]he consequences of a false indication by a sniffer dog can be severe" (*Chehil*, above, at paragraph 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.

précité, aux paragraphes 26 et 27; *Jarvis*, précité, aux paragraphes 61 et 62; *Colarusso*, précité, aux pages 52 et 53; et *McKinlay*, précité, aux pages 645 et 646). Cet équilibre doit être atteint dans le cadre de l'évaluation, dans son ensemble, si la fouille ou la perquisition est autorisée par la loi, du caractère raisonnable de la disposition législative l'autorisant et du caractère raisonnable de la méthode utilisée.

[225] Dans la trilogie des affaires de « chiens renifleurs » (*Kang-Brown*, *A.M.* et *Chehil*, précités), la Cour suprême a accordé beaucoup d'importance à la possibilité d'un contrôle judiciaire a posteriori des fouilles effectuées sans mandat afin d'en évaluer le caractère raisonnable. Toutefois, cela semble avoir été le cas en partie à cause des préoccupations concernant la fiabilité de certains chiens (*Chehil*, précité, aux paragraphes 25 et 48 à 54 et *A.M.*, précité, aux paragraphes 84 à 86 et 90), en partie « en raison de l'importance et de la qualité des renseignements qu'elle permet d'obtenir au sujet des contenus dissimulés dans les effets personnels d'un suspect ou sur sa personne » (*Kang-Brown*, précité, au paragraphe 58) et en partie parce que « [l]es conséquences d'un faux positif peuvent être graves » (*Chehil*, précité, au paragraphe 49).

[226] Ces affaires se distinguent de celles qui concernent l'utilisation, par le SCRS, de la technologie relative aux ESB pour recueillir l'IMSI et l'IMEI de l'appareil électronique sans fil d'une personne, car cette technologie est très fiable et ne peut donc pas entraîner d'éventuelles conséquences graves ayant trait à un « faux positif ». De plus, cette technologie brime beaucoup moins les droits d'une personne en matière de vie privée que le recours à un chien renifleur, qui peut permettre de tirer des conclusions avec une certaine certitude quant au contenu dissimulé notamment dans les bagages, le sac à main, le sac à dos ou la personne même d'un individu. En bref, l'IMSI et l'IMEI ne permettent d'établir aucune conclusion quant au *contenu* d'un appareil mobile ou à ce à quoi il permet d'accéder, pas plus qu'ils n'aident le SCRS à tirer des conclusions plausibles au sujet du contenu précis des communications effectuées au moyen d'un appareil mobile.

[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 paragraph 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 [***] 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 [***] 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

[227] La très grande fiabilité de la technologie relative aux ESB et la mesure dans laquelle elle brime le droit d'une personne au respect de sa vie privée, permet également de faire une distinction entre la présente instance et l'arrêt *Goodwin*, précité, au paragraphe 72, où la Cour a considéré que la non-disponibilité d'un contrôle judiciaire a posteriori dans le cadre d'un alcootest était un facteur très important, « surtout compte tenu des doutes concernant la fiabilité de [l'alcootest], de l'absence d'une étape intermédiaire entre l'analyse effectuée au moyen d'un [alcootest] et la suspension imposée lors d'un contrôle routier et de l'immédiateté des sanctions qui s'ensuivent ».

[228] En l'espèce, je crois que la nature des intérêts de l'État (sécurité nationale) est suffisamment importante pour que l'absence, dans la Loi sur le SCRS, de toute exigence en matière de contrôle judiciaire a posteriori pour chaque collecte d'IMSI et d'IMEI par le SCRS ne rende pas l'article 12 déraisonnable. C'est particulièrement le cas à cause de la nature minimale de l'atteinte, par le SCRS, au droit d'une personne au respect de sa vie privée, du fait que de telles atteintes sont autorisées par la disposition législative (c.-à-d. l'article 12) du fait que l'article 12 prévoit les différentes limites susmentionnées, d'autres mécanismes régulateurs dont je discuterai plus loin, et du fait qu'un mandat de la Cour est requis [***] Lorsque le SCRS demande un tel mandat, la Cour a l'occasion d'examiner le caractère raisonnable des motifs qu'a le SCRS de soupçonner que les activités de l'individu peuvent constituer des menaces envers la sécurité du Canada. Avant ce moment, les conséquences potentielles d'une fouille pour cet individu ne sont que très limitées, voire inexistantes.

[229] Je sais que ce contrôle judiciaire a posteriori prévu par la Loi sur le SCRS a lieu uniquement lorsque le SCRS décide de demander des pouvoirs conférés par des mandats contre une cible. Selon [***] L'IMSI et l'IMEI recueillies par la suite aident le SCRS à exécuter les mandats contre le bon appareil sans fil. Toutefois, lorsqu'aucun mandat n'a été décerné avant une opération fondée sur des ESB, il peut ne pas y avoir de contrôle judiciaire du caractère envahissant quant aux droits en matière de vie privée i) des cibles qui ne font pas l'objet d'une demande de mandat ou ii) de tiers. Néanmoins,

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 paragraph 53; *A.M.*, above, at paragraph 90; *Kang-Brown*, above, at paragraph 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

cette situation est sensiblement analogue à celle des chiens renifleurs susmentionnée. Dans ces affaires, un contrôle judiciaire a posteriori ne serait possible que si des procédures pénales étaient intentées contre un individu dont les bagages ou la personne, notamment, avaient fait l'objet d'une fouille par chien renifleur (*Chehil*, précité, au paragraphe 53; *A.M.*, précité, au paragraphe 90 et *Kang-Brown*, précité, au paragraphe 59). Partant, l'absence d'une certaine forme de contrôle judiciaire a posteriori pour *toutes* les fouilles minimalement envahissantes pouvant être effectuées en vertu d'une disposition législative ne semble pas, en soi, rendre celle-ci déraisonnable.

Présence d'autres « mécanismes régulateurs » ou mesures de responsabilisation

[230] En plus du contrôle judiciaire a posteriori qui, en vertu de la Loi sur le SCRS, doit avoir lieu si le Service désire établir un lien entre l'IMSI et l'IMEI tirées de l'appareil mobile d'un individu à son identité, la Loi sur le SCRS prévoit un certain nombre de mesures de responsabilisation ou « mécanismes régulateurs ».

[231] Plus précisément, le paragraphe 6(1) prévoit que le directeur du SCRS, « [s]ous la direction du ministre », est chargé de la gestion du Service et de tout ce qui s'y rattache. De plus, le paragraphe 6(2) précise que le ministre peut donner par écrit des instructions au directeur. La procureure générale souligne qu'une de ces instructions, qui porte sur les opérations et la responsabilisation, précise que les activités opérationnelles du SCRS doivent être raisonnables et proportionnelles à la menace, et que le Service doit tenter de minimiser les atteintes aux droits de la personne, dont au droit à la vie privée, dans la mesure du possible et conformément au droit canadien. Le paragraphe 6(4) exige également que le directeur du SCRS présente un rapport annuel au ministre concernant les activités opérationnelles ayant eu lieu au cours de l'exercice. Je crois qu'il est approprié de prendre connaissance d'office des déclarations publiques du ministre indiquant qu'il prend très au sérieux le rôle que lui confie l'article 6 de la Loi sur le SCRS.

[232] De plus, en vertu du paragraphe 20(2), « le directeur [du SCRS] fait rapport au ministre des actes qui

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.

peuvent avoir été accomplis selon lui illicitement, dans des cas particuliers, par des employés dans l'exercice censé tel des fonctions conférées au Service en vertu de la présente loi ». Je signale en passant que le paragraphe 20(3) prévoit en outre la présentation de tels rapports à la procureure générale.

[233] De plus, les activités du SCRS font l'objet d'un examen par le CSARS, qui a été constitué en vertu du paragraphe 34(1) de la Loi sur le SCRS. Les vastes fonctions du CSARS sont décrites au paragraphe 38(1). Il est notamment chargé de surveiller la façon dont le SCRS exerce ses fonctions. Conformément au paragraphe 20(4), tout rapport préparé par le directeur au titre du paragraphe 20(2) et présenté à la procureure générale au titre du paragraphe 20(3) doit également être remis au CSARS qui, selon le sous-alinéa 38(1)a)(iv), a pour mandat de l'examiner. Le CSARS est aussi chargé de présenter au ministre un certificat indiquant dans quelle mesure il est satisfait du rapport annuel du SCRS et signalant toute activité du SCRS visée dans le rapport qui, selon lui, i) n'est pas autorisée sous le régime de la Loi sur le SCRS ou contrevient aux instructions données par le ministre en vertu du paragraphe 6(2) ou ii) comporte un exercice abusif ou inutile par le SCRS de ses pouvoirs.

[234] Tel qu'indiqué au paragraphe 11 des présents motifs, la Cour a appris que le SCRS utilisait la technologie relative aux ESB lorsqu'elle a pris connaissance d'un des rapports classifiés du CSARS. Comme pour ce qui est de l'utilisation de métadonnées par le SCRS, révélée dans le même rapport, cela semble avoir poussé le SCRS, du moins en partie, à faire preuve d'une transparence accrue à l'égard de la Cour quant à son utilisation de la technologie relative aux ESB. Je crois qu'à cet égard, la surveillance par le CSARS des activités du SCRS en ce qui a trait aux métadonnées et à la technologie relative aux ESB s'est avérée essentielle.

[235] Selon moi, les rôles et les responsabilités du ministre, du CSARS et du directeur du SCRS, tel qu'ils sont décrits plus haut, permettent de s'assurer que l'article 12 est une disposition législative raisonnable lorsqu'il s'agit d'évaluer le caractère minimalement envahissant des fouilles qu'il autorise.

Conclusion Regarding the Reasonableness of Section 12

[236] Based on the foregoing assessment in Part VII.C.2.(b) 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 paragraph 23; *Tse*, above, at paragraph 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, analyze and retain information that ranges from non-intrusive to highly intrusive. However, the provisions in section 21 of the Act

Conclusion concernant le caractère raisonnable de l'article 12

[236] Selon l'évaluation effectuée à la partie VII.C.2)b), je conclus que l'article 12 est une disposition législative raisonnable. Selon moi, cette conclusion est étayée de la façon suivante.

i. *Nature et objet de l'article 12 :* L'article 12 confère au SCRS un rôle central, et sans doute essentiel, au sein de l'appareil de sécurité nationale du Canada. L'objectif du législateur au moment de conférer ce rôle au SCRS revêt une importance prédominante et est lié aux atteintes minimales qui sont autorisées en vertu de l'article 12 (*Chehil*, précité, au paragraphe 23 et *Tse*, précité, au paragraphe 21). Dans ce contexte, le critère des « motifs raisonnables de soupçonner » et l'absence d'autorisation judiciaire préalable sont justifiés, surtout lorsque i) l'atteinte minimale aux droits d'une personne en matière de vie privée est étroitement ciblée et très précise, comme l'utilisation que fait le SCRS de la technologie relative aux ESB, et ii) le SCRS détruit très rapidement les IMSI et les IMEI de tiers recueillies fortuitement, sans les avoir analysées, après qu'il a été confirmé qu'elles ne proviennent pas d'un appareil sans fil dont la cible est propriétaire ou qu'elle utilise. Les limites prévues à l'article 12 ainsi que dans la définition de « menaces envers la sécurité du Canada » figurant à l'article 2 de la Loi sur le SCRS permettent de s'assurer que l'article 12 n'a pas une portée excessive et qu'il n'est pas trop vague, et que les informations recueillies par le SCRS ont un lien rationnel avec le mandat qui lui est confié par l'article 12.

ii. *Mesure de l'atteinte autorisée par l'article 12 :* Les limites susmentionnées permettent de s'assurer que le SCRS n'est pas autorisé à effectuer des enquêtes envahissantes sur des personnes dont les activités sortent de ce cadre. Le SCRS peut recueillir, analyser et conserver des informations obtenues de façon non envahissante ou très envahissante au sujet des quelques activités qui s'inscrivent dans le cadre très étroit qu'établit l'article 12. Toutefois,

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

les dispositions de l'article 21 de la Loi sur le SCRS concernant les mandats prévoient que le SCRS ne peut pas mener, sans mandat, d'activités plus envahissantes.

iii. *Mesure dans laquelle la* Loi sur le SCRS *prévoit une supervision :* Le contrôle judiciaire prévu sous le régime de l'article 21 de la Loi sur le SCRS se déclenche dès que le SCRS tente d'obtenir les pouvoirs nécessaires pour mener, contre une personne, des activités d'enquête plus que minimalement envahissantes, dont l'obtention d'informations sur un abonné auquel des appareils mobiles ont été attribués par suite d'une opération fondée sur des ESB. À ce moment, la Cour a l'occasion d'évaluer, entre autres, le caractère raisonnable des motifs de soupçonner que les activités de cette personne peuvent constituer des menaces envers la sécurité du Canada. Un tel contrôle judiciaire a posteriori est sensiblement analogue à celui qui est déclenché dans d'autres contextes, et seulement après que des poursuites pénales ont été intentées contre la personne dont les droits en matière de vie privée ont été enfreints.

iv. La Loi sur le SCRS donne au CSARS un rôle important de contrôle qu'il assume. De plus, la Loi sur le SCRS précise que le directeur du SCRS, «[s]ous la direction du ministre», est chargé de la gestion du Service et de tout ce qui s'y rattache. Le directeur a également des obligations en matière de reddition de comptes au ministre, dont la production d'un rapport annuel à l'intention du Parlement. De plus, le ministre a le pouvoir de donner des instructions écrites au directeur, et l'une d'elles impose au directeur des contraintes importantes dont la portée va au-delà de ce qui est prévu à l'article 12.

iii) La fouille a-t-elle été effectuée de manière abusive?

[237] L'essentiel de la preuve produite en l'espèce concerne plutôt la façon dont les opérations fondées sur

conducted relates to CSS operations generally, rather than to the specific CSS operation that was conducted in respect of [***]

[238] In addition, the IMSI and IMEI information that was captured from third parties at the time of CSIS's CSS operations against [***] 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. [***] In view of the fact that I am addressing various issues relating to those types of powers in [***] 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, [***] testified that CSIS's equipment maintains contact with mobile devices [***] Based on the fact that an average telephone call from a mobile device typically takes approximately five to fifteen seconds to go through, and will persist in trying to connect a call for "up to tens of seconds", [***] has testified that CSS operations have no discernible adverse impact on the experience of a user of a mobile device. For greater certainty, [***] 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. [***] testified that CSIS has a policy of not capturing such content.

des ESB s'effectuent en général que le déroulement de l'opération ayant visé [***]

[238] De plus, les IMSI et les IMEI de tiers recueillies lors des opérations fondées sur des ESB menées par le SCRS contre les appareils de [***] ont été détruites avant de faire l'objet de la moindre analyse et ne faisaient pas partie du rapport opérationnel préparé par le SCRS. [***] Dans la mesure où j'aborde différentes questions relatives à ces pouvoirs dans le dossier [***], qui est en voie d'être publié en même temps que la présente décision, je m'abstiendrai de faire d'autres commentaires sur le sujet dans les présents motifs.

[239] La preuve produite en l'espèce a davantage trait aux opérations fondées sur des ESB du SCRS en général. Plus particulièrement, [***] a témoigné que le matériel du SCRS permet de garder le contact avec des appareils mobiles [***] Puisque l'acheminement d'un appel téléphonique moyen fait à partir d'un appareil mobile prend environ de cinq à quinze secondes et que l'appareil continuera de tenter d'établir le contact pendant plusieurs dizaines de secondes, [***] a témoigné que les opérations fondées sur des ESB ne nuisent d'aucune manière perceptible à l'expérience de l'utilisateur d'un appareil mobile. Je précise que [***] a soutenu que les ESB du SCRS et le matériel connexe n'interrompent pas un appel actif.

[240] De plus, les opérations du SCRS fondées sur des ESB n'ont pas d'incidence sur la capacité de l'utilisateur de l'appareil mobile de composer le 911, car le premier réseau légitime de toute région qui reçoit un tel appel l'acheminera, même si la tour est exploitée par un autre FST que celui de l'utilisateur.

[241] De plus, à une exception près, les ESB du SCRS et le matériel connexe ne peuvent pas intercepter le contenu d'une communication ou obtenir des informations stockées dans un appareil mobile. [***] a témoigné que le SCRS a pour politique de ne pas recueillir un tel contenu.

[242] Finally, [***] testified that CSIS deletes the IMSI and IMEI information that it captures from the mobile devices of third parties very quickly, often within [***] 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, [***] 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 paragraph 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.

[242] Enfin, selon [***] le SCRS élimine très rapidement les IMSI et les IMEI tirées d'appareils mobiles de tiers, souvent dans les [***] jours suivant la collecte et, de toute façon, dès qu'un rapport a été rédigé sur l'opération ou l'ensemble d'opérations fondées sur des ESB. De plus, les IMSI et les IMEI pour lesquels il a été établi qu'elles n'ont pas de lien avec les appareils mobiles visés par l'opération fondée sur des ESB, [***] ne font l'objet d'aucune analyse.

[243] Compte tenu de tout ce qui précède, je suis convaincu que la façon dont le SCRS mène ses opérations fondées sur des ESB n'est pas abusive.

iv) Conclusion concernant le caractère raisonnable de l'utilisation, par le SCRS, de la technologie relative aux ESB

[244] Pour les motifs résumés aux parties VII.C.2)b)i) à iii), je conclus que l'utilisation, par le SCRS, de la technologie relative aux ESB pour recueillir les IMSI et les IMEI des appareils mobiles d'une cible d'une enquête est autorisée par l'article 12 de la Loi sur le SCRS, que cet article est une disposition législative raisonnable et que la façon dont le SCRS mène actuellement ses opérations fondées sur des ESB n'est pas abusive. En tirant ces conclusions, j'ai tenu compte du besoin d'adopter une « approche téléologique axée principalement sur la protection de la vie privée considérée comme une condition préalable à la sécurité individuelle, à l'épanouissement personnel et à l'autonomie ainsi qu'au maintien d'une société démocratique prospère » (*Spencer*, précité, au paragraphe 15).

[245] M'appuyant sur ces constatations, je conclus au caractère raisonnable de cette activité, de la façon dont le SCRS la mène. En d'autres termes, je suis d'accord avec la constatation du CSARS, selon qui le SCRS n'a pas besoin de mandat pour la mener, pourvu qu'elle le soit de la façon décrite ci-dessus. Je remarque que, même s'ils en sont arrivés à une conclusion contraire, les *amici* ont observé que cette activité se trouvait tout juste au-delà du seuil marquant la nécessité d'un mandat. Ils ont ajouté que la conclusion contraire pouvait raisonnablement être tirée.

[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 [***] 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 [***] |[***] and communications patterns", with the aid of information already available to CSIS. This engaged [***] 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

[246] Cette conclusion repose largement sur les éléments de preuve présentés en l'espèce concernant la façon dont le SCRS mène actuellement ses opérations fondées sur des ESB ainsi que les fonctions actuelles des ESB du SCRS et du matériel connexe. Je m'attends à ce que les mesures que j'ai indiquées en concluant que la collecte d'IMSI et d'IMEI par le SCRS était minimalement envahissante, donc légale, fassent l'objet d'un examen minutieux par le ministre et le CSARS lorsqu'ils étudieront l'utilisation, par le SCRS, de la technologie relative aux ESB.

VIII. Conclusion

[247] Pour les motifs susmentionnés, l'utilisation, par le SCRS, de la technologie relative aux ESB pour recueillir sans mandat les identificateurs que sont les IMSI et les IMEI des appareils sans fil de [***] était visée par l'article 8 de la Charte, car cette activité constituait une fouille. La collecte, par le SCRS, des IMSI et des IMEI des appareils sans fil de [***] constituait une fouille, car elle a aidé le SCRS à dresser un profil de [***] entre autres en lui permettant éventuellement d'esquisser ses [***] et ses habitudes de communication à l'aide des informations dont il dispose déjà. En permettant de contourner l'anonymat de son utilisation de ses appareils mobiles, qui est de nature très personnelle, cette activité a mis en cause les droits de [***] garantis par l'article 8 de la Charte.

[248] Toutefois, cette activité n'était pas abusive au sens de l'article 8 et, partant, n'était pas illégale.

[249] La raison en est que ces fouilles étaient étroitement ciblées, très précises et minimalement envahissantes, principalement grâce aux mesures mises en œuvre par le SCRS dans le cadre de ses opérations fondées sur des ESB. Si ces mesures n'avaient pas été adoptées par le SCRS, j'aurais pu en arriver à une conclusion différente.

[250] Toutefois, les fouilles n'étaient pas abusives, car les ESB du SCRS et le matériel connexe ne permettaient en aucune façon d'accéder aux appareils mobiles, à leur contenu ou à ce qu'ils permettaient de consulter. De plus,

CSIS's CSS equipment. Moreover, with the one exception [***] 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 [***] Based on the fact that an average telephone call from a mobile device typically takes approximately five to fifteen 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 [***] 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, [***] 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, at paragraph 51). These steps are also critical to ensuring that there is a meaningful nexus between the individual(s) whose information is retained and analyzed by CSIS, and the threat to the security of Canada contemplated by section 12.

à une exception près [***] ce matériel ne permet pas d'accéder au contenu des communications effectuées au moyen d'appareils mobiles. Le SCRS a assuré la Cour qu'il n'utilise pas ses ESB ni le matériel connexe pour avoir accès à un tel contenu.

[251] De plus, le matériel du SCRS garde le contact avec les appareils mobiles [***] Selon des éléments de preuve qui n'ont pas été contestés, un appel téléphonique moyen effectué à partir d'un appareil mobile prend environ de cinq à quinze secondes avant d'être acheminé, et l'appareil continuera de tenter d'établir le contact pendant des dizaines de secondes. Partant, les opérations du SCRS fondées sur des ESB ne nuisent d'aucune manière perceptible à l'expérience de l'utilisateur d'un appareil mobile. De plus, les opérations du SCRS fondées sur des ESB n'ont pas d'incidence sur la capacité de l'utilisateur de l'appareil mobile de composer le 911, car le premier réseau légitime de toute région qui reçoit un tel appel l'acheminera, même si la tour est exploitée par un autre FST que celui de l'utilisateur.

[252] Enfin, le SCRS supprime très rapidement les IMSI et les IMEI tirées d'appareils mobiles de tiers, souvent dans les [***] jours suivant la collecte et, de toute façon, dès qu'un rapport a été rédigé sur l'opération ou l'ensemble d'opérations fondées sur des ESB. De plus, les IMSI et les IMEI pour lesquelles il a été établi qu'elles n'ont pas de lien avec les appareils mobiles visés par l'opération fondée sur des ESB, [***] ne font l'objet d'aucune analyse.

[253] Selon moi, la destruction rapide des IMSI et des IMEI de tiers et la politique du SCRS visant à n'effectuer aucune autre analyse de ces informations sont, ensemble, des mesures essentielles pour s'assurer qu'une opération fondée sur les ESB est raisonnable et n'a pas une portée excessive (*Chehil*, précité, au paragraphe 51). Ces mesures sont également essentielles pour s'assurer qu'il existe un lien significatif entre la personne dont le SCRS conserve et analyse les informations et la menace envers la sécurité du Canada dont il est question à l'article 12.

[254] The retention of third party IMSI or IMEI information beyond a very short period of time, or the analysis of such information for a purpose other than simply assisting to identify the mobile device(s) of a subject of investigation, is not authorized by section 12. For this purpose, a "very short period of time" would be measured in days or weeks, although I will remain open to being persuaded that there are sound reasons for aligning this period with the [***] for the destruction of third party information that is applicable in other contexts, including the retention of certain types of metadata (*X (Re)*, above, at paragraph 253). I expect that this will be the subject of further exchanges with the Attorney General following the release of this decision.

[254] L'article 12 n'autorise pas la conservation d'IMSI ou d'IMEI de tiers au-delà d'un très court laps de temps ou leur analyse à des fins autres que la simple reconnaissance de l'appareil mobile d'une cible. À cette fin, un « très court laps de temps » se mesure en jours ou en semaines, bien que je demeure disposé à me laisser convaincre qu'il existe de bonnes raisons pour faire correspondre cette période avec le délai [***] qui s'applique à l'élimination des informations sur des tiers en d'autres contextes, dont la conservation de certains types de métadonnées (*X (Re)*, précité, au paragraphe 253). Je prévois que cette question fera l'objet d'autres échanges avec la procureure générale après la publication de la présente décision.

[255] I also consider it to be significant [***]

[255] J'accorde aussi de l'importance à [***]

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

[256] J'ajouterai simplement trois autres conclusions.

[257] First, CSIS should not be relying on the language of [***] 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.

[257] Premièrement, le SCRS ne doit pas s'appuyer sur le libellé du [***] ou de tout autre mandat pour mener une quelconque opération fondée sur des ESB. S'il souhaite obtenir un mandat pour effectuer de telles opérations, le SCRS doit le demander en termes explicites.

[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.

[258] Deuxièmement, s'il désire utiliser des informations obtenues directement ou indirectement lors d'une opération fondée sur des ESB, le SCRS doit s'assurer, dans toute prochaine demande de mandat présentée à la Cour, de préciser à celle-ci les informations suivantes, qui ont trait à la preuve fournie en l'espèce : i) toute modification apportée à la façon dont le Service a mené ses opérations fondées sur des ESB, ii) toute modification apportée aux capacités du matériel utilisé dans le cadre de telles opérations et iii) toute modification apportée à l'objectif visé par l'utilisation du matériel.

[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 paragraphs 26 and 75).

[259] Troisièmement, je crois que l'article 12 n'autorise pas l'utilisation de la technologie relative aux ESB pour recueillir en « lots » les IMSI et les IMEI des appareils mobiles du public. Compte tenu de la nature hypothétique d'une telle opération, elle ne satisferait pas au critère d'une fouille sans mandat (*Kang-Brown*, précité, aux paragraphes 26 et 75).

JUDGMENT in [***]

THIS COURT'S JUDGMENT is that CSIS's warrantless use of CSS technology to capture the identifying characteristics of [***] mobile devices was not unlawful. It did not contravene the *Radiocommunication Act*, R.S.C., 1985, c. R-2, the *Criminal Code*, R.S.C., 1985, c. C-46 or section 8 of the *Canadian Charter of Rights and Freedoms*, being Part I of the *Constitution Act*, 1982, Schedule B, *Canada Act 1982*, 1982, c. 11 (U.K.) [R.S.C., 1985, Appendix II, No. 44]. Although CSIS's use of a CSS against [***] 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 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.

JUGEMENT relatif au dossier [***]

LA COUR STATUE que le SCRS n'a pas agi dans l'illégalité en utilisant, sans mandat, la technologie relative aux ESB pour recueillir les caractéristiques distinctives des appareils mobiles de [***] Cela ne contrevenait ni à la *Loi sur la radiocommunication*, L.R.C. (1985), ch. R-2, ni au *Code criminel*, L.R.C. (1985), ch. C-46, ni à l'article 8 de la *Charte canadienne des droits et libertés*, qui constitue la partie I de la *Loi constitutionnelle de 1982*, annexe B, *Loi de 1982 sur le Canada*, 1982, ch. 11 (R.-U.) [L.R.C. (1985), appendice II, nº 44]. Même si l'utilisation d'un ESB contre [***] constituait une fouille, celle-ci n'était pas abusive, car elle était étroitement ciblée, très précise et minimalement envahissante.

Dans les sept jours suivant la date du présent jugement et des motifs qui l'accompagnent, les *amici curiae* et la procureure générale les passeront en revue pour déterminer les parties qui peuvent être rendues publiques. Les *amici curiae* et la procureure générale se consulteront et prendront des décisions en fonction du principe de la publicité des débats judiciaires. Toute question litigieuse doit être soumise à mon attention ou à celle d'un juge désigné, advenant le cas où je ne suis pas en mesure d'exercer ma fonction judiciaire.

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

SECRET

SECRET

ANNEXE I

[TRADUCTION]

PIÈCE « C »

POUVOIR D'UTILISER LA RADIO

1) Aux termes du sous-alinéa 5(1)a)(v) de la *Loi sur la radiocommunication*, la présente constitue une autorisation pour le Service canadien du renseignement de sécurité (SCRS) relativement à tous les types d'appareils radio spécialement conçus aux fins indiquées au paragraphe 2, à l'égard desquels une licence radio, délivrée en vertu du sous-alinéa 5(1)a)(i) de la *Loi sur la radiocommunication*, n'est pas indiquée.

2) La présente autorisation s'applique aux appareils radio décrits au paragraphe 1 seulement quand ils sont mis à l'essai ou quand ils sont utilisés à des fins de formation ou à des fins d'activités opérationnelles dans le cadre des enquêtes menées en vertu des articles 12 et 16 de la *Loi sur le Service canadien du renseignement de sécurité*, LRC 1985, ch C-23.

3) Les appareils radio décrits au paragraphe 1, utilisés aux fins indiquées au paragraphe 2, ne sont pas assujettis au paragraphe 4(2) de la *Loi sur la radiocommunication*, lequel prévoit que les appareils radio nécessitent un certificat d'approbation technique du ministère.

4) Les appareils radio décrits au paragraphe 1, utilisés aux fins indiquées au paragraphe 2, ne sont pas assujettis au paragraphe 4(3) de la *Loi sur la radiocommunication*, aux termes duquel les appareils radio doivent être conformes aux normes techniques fixées par le ministère.

5) La présente autorisation n'écarte pas l'exigence d'obtenir la licence d'une station de radiocommunication ou l'autorisation exigée en vertu de la *Loi sur la radiocommunication* relativement aux appareils radio utilisés à des fins non prévues au paragraphe 2.

6) La présente autorisation ne s'applique pas aux appareils radio à l'égard desquels aucune licence radio n'est exigée, ou à l'égard desquels une licence ou une autorisation a été accordée en vertu de la *Loi sur la radiocommunication*.

7) Aucun appareil radio visé par la présente autorisation ne devra causer une interférence nuisible à d'autres appareils radio faisant l'objet d'une autorisation ou d'une licence.

8) Aucune protection n'est accordée aux appareils radio visés par la présente autorisation contre les effets d'une interférence.

9) La présente autorisation est valide à moins d'être retirée par le ministère des Communications ou à moins que le Service canadien du renseignement de sécurité (SCRS) indique par écrit qu'elle n'est plus nécessaire.

Original signed by/
Original signé par
Perrin Beatty

Perrin Beatty
Ministre des Communications

Date : 1er sept. 1992

APPENDIX II

Innovation, Science and Economic Developrnent Canada / Innovation, Sciences et Développement économique Canada

Our File: 49081700428

MAR 1 3 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,

Peter Hill
Director General
Spectrum Management Operations Branch

Attachment

ANNEXE II

[TRADUCTION]

Notre dossier : 49081700428

LE 13 MARS 2017

M. Peter Henschel
Sous-commissaire
Services de police spécialisés
Gendarmerie royale du Canada
273, promenade Leikin
Ottawa (Ontario) K1A 0R2

M. Henschel,

La présente lettre constitue une autorisation, délivrée en vertu du sous-alinéa 5(1)a)(v) de la *Loi sur la radiocommunication*, pour les employés de la Sous-direction des services d'enquêtes techniques de la Gendarmerie royale du Canada (GRC), ainsi que pour les employés de la GRC qui relèvent de cette sous-direction. Cette autorisation s'applique seulement à l'installation, au fonctionnement et à la possession d'appareils radio conçus pour communiquer avec des appareils mobiles sur les réseaux mobiles commerciaux dans le but d'obtenir les données associées à un appareil mobile ou au réseau mobile qui, conformément à l'article 492.2 du *Code criminel :*

a) concernent les fonctions de composition, de routage, d'adressage ou de signalisation en matière de télécommunication;

b) soit sont transmises pour identifier, activer ou configurer un dispositif, notamment un programme d'ordinateur au sens du paragraphe 342.1(2) du Code criminel, en vue d'établir ou de maintenir l'accès à un service de télécommunication afin de rendre possible une communication, soit sont produites durant la création, la transmission ou la réception d'une communication et indiquent, ou sont censées indiquer, le type, la direction, la date, l'heure, la durée, le volume, le point d'envoi, la destination ou le point d'arrivée de la communication;

c) ne révèlent pas la substance, le sens ou l'objet de la communication.

La présente autorisation est assujettie aux modalités ci-jointes et expire cinq ans après la date à laquelle elle est signée. Plus particulièrement, il est possible d'installer, de faire fonctionner ou de posséder ces appareils radio seulement aux fins indiquées à l'article 54 du *Règlement sur la radiocommunication*.

Veuillez agréer, Monsieur, l'expression de mes sentiments les meilleurs.

Peter Hill
Directeur général
Direction générale des opérations de la gestion du spectre

Pièce jointe

APPENDIX III

Canadian Security Intelligence Service Act, R.S.C., 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*)

…

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.

ANNEXE III

Loi sur le Service canadien du renseignement de sécurité, L.R.C. (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*)

[…]

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.

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 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

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.

Mesures 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, 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

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 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

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

(b) any person other than

(i) a Canadian citizen,

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

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

Limitation

(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).

Personal consent of Ministers required

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

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

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

…

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

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

(i) les citoyens canadiens,

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

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

Restriction

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

Consentement personnel des ministres

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

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

b) au consentement personnel écrit du ministre.

[…]

Judicial Control

Application for warrant

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

(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;

Contrôle judiciaire

Demande de mandat

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

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

Activities outside 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.

Matters to be specified in warrant

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

(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;

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

Activités à l'extérieur du 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.

Contenu du mandat

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

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;

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

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

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

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

Maximum duration of warrant

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

(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.

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) les personnes ou catégories de personnes destinataires du mandat;

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

e) la durée de validité du mandat;

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

Durée maximale

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

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.

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 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 section 19 of the *Citizenship Act*, and

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 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 l'article 19 de la Loi sur la citoyenneté,

(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, R.S.C., 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 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

(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, L.R.C. (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 sur les cas concernant la présence des dossiers dans chacun desquels dominent 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.

National Capital Region described in the schedule to the *National Capital Act*.

Radiocommunication Act, R.S.C., 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,

(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;

Loi sur la radiocommunication, L.R.C. (1985), 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) 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) 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 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).

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 réseau ainsi décodé;

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

Criminal Code, R.S.C., 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 electro-magnetic, 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

(a) a person who has the consent to intercept, express or implied, of the originator of the private

Code criminel, L.R.C. (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) une personne qui a obtenu, de l'auteur de la communication privée ou de la personne à laquelle son

communication or of the person intended by the originator thereof to receive it;

(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;

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

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

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

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

(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

(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 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).

auteur la destine, son consentement exprès ou tacite à l'interception;

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

(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) 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) 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) 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-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).

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).

…

429 ….

Colour of right

(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.

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).

[…]

429 […]

Apparence de droit

(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.