Federal Court Cour fédérale

TRÈS SECRET

Date : 20170927

Dossier : CONF-2-17

Citation : 2017 CF 1047

Ottawa (Ontario), ce 27e jour de septembre 2017

EN PRÉSENCE DU JUGE EN CHEF

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

et

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

JUGEMENT ET MOTIFS PUBLICS

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*, Partie I de la *Loi constitutionnelle de 1982*, annexe B de la *Loi de 1982 sur le Canada* (Royaume-Uni), ch 11 [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, [redacted] Cette activité comprenait l'utilisation d'un émulateur de station de base [ESB] pour obtenir les caractéristiques distinctives des appareils mobiles de [redacted], et ce, sans mandat.

[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 [redacted] 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 [redacted] 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 [redacted] 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*, LRC (1985), ch R-2, au *Code criminel*, LRC 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 [redacted] 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 [redacted] 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 [redacted] relativement aux informations que le SCRS, en ayant accès aux IMSI et 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 [redacted] notamment en lui permettant éventuellement de mieux connaitre ses [redacted] 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 [redacted] 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 [redacted]

[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 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*, LRC (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 n^{o} 2014-03 : Utilisation des métadonnées par le 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 [*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 [redacted] le SCRS l'a utilisée de plus en plus, au point où il s'en sert maintenant d'un océan à l'autre, [redacted]

[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 [redacted] Pour ce faire, le SCRS utilise la technologie relative aux ESB pour obtenir l'IMSI liée à la carte SIM 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 [redacted] 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 [redacted] 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 [redacted] par [redacted] un employé de niveau supérieur du SCRS, à l'audition de la preuve relative à la présente demande.

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

[17] Par la suite, lors d'une conférence de gestion d'instance [redacted] que j'ai coprésidée le [redacted] 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[1]. 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 [redacted] 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] [redacted] Ainsi, la Cour a appris que le SCRS utilisait des ESB ou des technologies similaires dans l'exécution de ses mandats.

[19] [redacted]

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

[20] Le [redacted] 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 [redacted] 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.

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 [redacted] Comme je l'explique plus loin, j'ai décerné les mandats en question, avec deux modifications, pour la période du [redacted] au [redacted]

[22] [redacted]

[redacted]

[23] Les IMSI et les IMEI obtenues des appareils sans fil de [redacted] en [redacted] ont aidé le SCRS à exercer les pouvoirs d'interception accordés par la Cour en [redacted] 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 [redacted] [affidavit [redacted] et de [redacted] [affidavit [redacted]. 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] [redacted]

[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 [redacted] contre

[redacted] qui devaient expirer [redacted] En premier lieu, j'ai ajouté un passage interdisant le recours aux ESB [redacted] au paragraphe [redacted] du mandat [redacted] Cette interdiction a été ajoutée à plusieurs autres mandats depuis que la Cour a appris que le SCRS s'appuyait sur le paragraphe [redacted] pour utiliser les ESB et [redacted] 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 [redacted]

[27] La seconde modification que j'ai apportée aux mandats demandés en l'espèce a été d'éliminer l'autorisation demandée d'obtenir des [redacted] 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 [redacted]

[28] Le [redacted] 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 [redacted] 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 [redacted] 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 [redacted] Pour les obtenir, le SCRS a utilisé différentes méthodes d'enquête, dont la filature et la réalisation d'interceptions en vertu de mandats contre [redacted] 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 [redacted] Ces informations ont été recueillies pendant deux jours et consistent uniquement en l'attribution de trois appareils à [redacted] à savoir [redacted] 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 [redacted] j'ai bien précisé que je restais saisi de la demande afin (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 [redacted] la procureure générale a confirmé que le libellé du [redacted] a uniquement été invoqué dans [redacted] instances, soit [redacted] 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 [redacted] notamment lors du contre-interrogatoire par les *amici*. À mon avis, il était aussi important qu'ils profitent des réponses de [redacted] 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 [redacted] 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] 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 [redacted] 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 [redacted] 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 [redacted] 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, LRC (1985), ch C-23	*Canadian Security Intelligence Service Act*, RSC 1985, c C-23
27. Une demande de mandat faite en vertu des articles 21, 21.1 ou 23, de renouvellement de mandat faite en vertu des articles 22 ou 22.1 ou d'ordonnance présentée au titre de l'article 22.3 est entendue à huis clos en conformité avec les règlements d'application de l'article 28.	27. An application under section 21, 21.1 or 23 for a warrant, an application under section 22 or 22.1 for the renewal of a warrant or an application for an order under section 22.3 shall be held in private in accordance with regulations made under section 28.

[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, au paragraphe 34.

> [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* (Brian A. Garner, 8e édition, St-Paul, Thomson West, 2004), et par *private* et « huis clos » dans le *Dictionnaire de droit québécois et canadien* (Hubert Reid, Montréal, Wilson et 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 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, 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, www.cbc.ca).

[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 [*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 d'*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] 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 (Procureur général)*, 2002 CSC 75 [*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*, LRC (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 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 *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 [redacted] dans son affidavit et de vive voix le [redacted] lors de l'audition de la preuve.

[52] [redacted] est [redacted] au SCRS. Son témoignage ne traitait pas du cas de [redacted] en particulier, mais plutôt de la technique en général. Il se décrit entre autres comme un spécialiste de la technologie relative aux ESB. [redacted] 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] [redacted] 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, [redacted]

[54] [redacted] a confirmé que le SCRS utilise la technologie relative aux ESB uniquement aux deux fins recensées 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] [redacted] 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, [redacted] 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 [contacts] et les habitudes de communication [redacted]

[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. [redacted]

a précisé que le SCRS ne cherche pas à géolocaliser quiconque sans mandat au moyen d'une opération fondée sur des ESB.

[57] Selon [redacted] 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 [redacted] 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. 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] [redacted] 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, [redacted] 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] [**information technique**]

[61] **[Information technique]**

[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. **[information technique]**

[63] **[information technique]**

[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] **[information technique]**

[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, **[information technique]**

[67] **[information technique]**

[68] **[information technique]** [redacted]

[69] **[information technique]** [redacted]

[70] **[information technique]** [redacted]

[71] **[information technique]** [redacted]

[72] [redacted] 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. [redacted]

[redacted] **[information technique]** [redacted]

[73] [redacted] 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. [redacted]

[2]

[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

[2] 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.

[redacted]

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

[78] Selon [redacted] 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. [redacted]

[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 [redacted] les rapports opérationnels sont généralement préparés dans [redacted] 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 [redacted] 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 *X (Re)*, précité, 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. [redacted]

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. *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.

> [TRADUCTION]
>
> 1) Aux termes du sous-alinéa 5(1)*a*)(v) de la *Loi sur la radiocommunication*, le présent document constitue, pour le Service canadien du renseignement de sécurité (SCRS), une autorisation relative à tout type d'appareil radio spécialement conçu et utilisé aux fins mentionnées au paragraphe 2, auquel une licence radio visée au sous-alinéa 5(1)*a*)(i) de la *Loi sur la radiocommunication* ne convient pas.
>
> 2) La présente autorisation s'applique aux appareils radio mentionnés au paragraphe 1 uniquement lorsqu'ils sont mis à l'essai ou utilisés à des fins de formation ou lors d'opérations, et ce, uniquement dans le cadre d'enquêtes menées au titre des articles 12 et 16 de la *Loi sur le service*

> *canadien du renseignement de sécurité*, LRC (1985), chap. C-23.
>
> […]
>
> 7) Les appareils radio visés par la présente autorisation ne seront source d'aucun brouillage préjudiciable pour d'autres appareils radio faisant l'objet d'une autorisation ou d'une licence.
>
> […]
>
> 9) La présente autorisation demeure valide jusqu'à ce que le ministère des Communications la retire ou que le Service canadien du renseignement de sécurité (SCRS) signifie par écrit qu'elle n'est plus nécessaire.
>
> [Non souligné dans l'original.]

[86] Le texte complet de l'Autorisation figure à l'annexe 1 des présents motifs.

[87] Les *amici* soulignent que le SCRS n'a pas eu accès à la technologie relative aux ESB [redacted] 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 2 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 « relative à tout type d'appareil radio spécialement conçu et utilisé aux fins mentionnées 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] 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, LRC, ch R-2	*Radiocommunication Act*, RSC, 1985, c R-2
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.	[harmful interference means] an adverse effect of electromagnetic energy from any emission, radiation or induction that (a) endangers the use or functioning of a safety-related telecommunication system, or (b) significantly degrades or obstructs, or repeatedly interrupts, the use or functioning of radio apparatus or radio-sensitive equipment.

[93] 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 *R. c Brewster*, 2016 ONSC 4133, aux paragraphes 34, 38, 51 et 52. Toutefois, les extraits de 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 [redacted] [maintient un contact avec un appareil mobile pendant quelques secondes] [redacted] À mon avis, [redacted] 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 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. [redacted]

[redacted]

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

Code criminel, LRC (1985), ch C-46	*Criminal Code*, RSC 1985, c C-46
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 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.

[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] 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] 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] Voici le paragraphe 430(1).

Code criminel, LRC (1985), ch C-46	*Criminal Code*, RSC 1985, c C-46
430 (1) Commet un méfait quiconque volontairement, selon le cas :	430 (1) Every one commits mischief who wilfully
a) détruit ou détériore un bien;	(a) destroys or damages property;
b) rend un bien dangereux, inutile, inopérant ou inefficace;	(b) renders property dangerous, useless, inoperative or ineffective;
c) empêche, interrompt ou gêne l'emploi, la jouissance ou l'exploitation légitime d'un bien;	(c) obstructs, interrupts or interferes with the lawful use, enjoyment or operation of property; or
d) empêche, interrompt ou gêne une personne dans l'emploi, la jouissance ou l'exploitation légitime d'un bien.	(d) obstructs, interrupts or interferes with any person in the lawful use, enjoyment or operation of property.

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

[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, au paragraphe 15 [*Spencer*]).

(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 RCS 425, à la page 505 [*Thomson Newspapers*] et *R. c McKinlay Transport Ltd*, [1990] 1 RCS 627, à la page 642 [*McKinlay*]).

[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. 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, au paragraphe 38 [*A.M.*]).

[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, au paragraphe 26 [*Tessling*]). 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 RCS 281, à la page 293 [*Plant*] 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, au paragraphe 27 [*Patrick*]).

[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] 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] 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. 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 RCS 8, au paragraphe 40 [*Evans*] et *R. c Colarusso*, [1994] 1 RCS 20, à la page 53 [*Colarusso*]), 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 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 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, au paragraphe 62 [*Jarvis*]). 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 RCS 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 RCS 145, aux pages 159 et 160 [*Hunter*]). 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, au paragraphe 21 [*Tse*]).

[127] En bref, l'endroit « où se situe la ligne de démarcation entre ce qui est abusif et ce qui ne l'est pas […] dépend de l'importance de l'objectif 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, au paragraphe 27 [*Rodgers*] 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, au paragraphe 56 [*Goodwin*] 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, au paragraphe 23 [*Chehil*]). À titre d'exemple, un degré élevé de fiabilité peut justifier l'imposition d'une norme judiciaire moins rigoureuse, par 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, aux paragraphes 25, 60, 210 et 213 [*Kang-Brown*] 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, au paragraphe 35 [*Mahjoub*]).

[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, au paragraphe 41 [*Wakeling*], *Rodgers*, précité, au paragraphe 25 et *R. c Collins*, [1987] 1 RCS 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 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 [redacted] 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 [redacted] 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 [redacted] afin de permettre au SCRS de reconnaître ces appareils et de les lui attribuer.

[138] Selon [redacted] les cibles d'une opération fondée sur des ESB sont habituellement connues [redacted] Il est donc important de garder à l'esprit qu'en général, le SCRS possède déjà des informations sur ces personnes à ce moment. Par exemple, il sait où elles se trouvent, [redacted] même s'il ignore peut-être leurs [redacted]

[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. [redacted] 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 [redacted] révélé [redacted]

[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, [redacted] employé de niveau supérieur du SCRS, [redacted] 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.] [redacted]

[144] Même si [redacted] 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 [redacted] Il est possible que ce soit ce dont parlait [redacted] lorsqu'il a témoigné que l'IMSI et l'IMEI sont nécessaires « pour déterminer les [contacts] les habitudes de communication et de nombreux autres éléments relatifs à des enquêtes en cours en matière de sécurité nationale ». [redacted]

[redacted] 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 n^{o} 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, à la page 15 [*Gone Opaque*]).

[146] Je souligne également que [redacted] 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 [redacted] 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, [redacted] 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 [redacted] 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 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 [contacts] 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, [redacted] 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, [redacted] (*Spencer*, précité, aux paragraphes 42 à 49).

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

[152] Selon [redacted] 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 [redacted] 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, [redacted] 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] [redacted]

[154] [redacted]

[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 [redacted]

[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 [redacted] **[pendant quelques secondes]** [redacted]

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 [redacted] 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 [redacted] jours, et certainement dès qu'un rapport opérationnel a été rédigé.

[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, [redacted]

[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 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 [redacted] le SCRS ne peut pas avoir accès au contenu des communications effectuées au moyen de l'appareil mobile.

[162] [redacted] de commencer à dresser un profil initial des [contacts] 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. [redacted]

[163] Alors que le SCRS peut commencer à dresser un profil initial des [contacts] 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. [redacted]

[redacted]

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 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] 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] 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] 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, au paragraphe 53 [*Charkaoui II*]), 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, [redacted] 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 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 RCS 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 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 [contacts] et habitudes de communication » [redacted] (ii) tirer des conclusions quant à [ces personnes] [redacted] 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 *X (Re)*, aux paragraphes 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, [redacted] 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. [redacted]
>
> (*X (Re)*, précité, au paragraphe 42.)

[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] 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] 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 *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 *Gomboc*, la Cour a accordé une importance considérable au fait que l'alinéa 10(3)f) du *Code of Conduct Regulation* adopté en vertu de la *Electric Utilities Act*, S.A. 2003, ch. E-5.1, permettait la divulgation d'informations sur le client aux agents de la paix aux fins d'une enquête sur une infraction, si cette divulgation n'allait pas à l'encontre de la demande expresse de ce dernier. 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 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://fr.wikipedia.org/wiki/International_mobile_subscriber_identity>).

[180] Bien que rien n'atteste [redacted] les *amici* ont indiqué que les éléments de preuve présentés par [redacted] 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. [redacted] Toutefois, compte tenu des éléments de preuve présentés par [redacted] selon lesquels [redacted], je ne crois pas que la conclusion des *amici* quant à ce point soit solide.

[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 *X (Re),* aux paragraphes 161 et 162.

> [161] 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*) [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.]
> >
> > (Sénat du Canada, Comité sénatorial spécial sur le Service canadien du renseignement de sécurité, *Équilibre délicat : un service du renseignement de sécurité dans une société démocratique* [novembre 1983] [Président : P.M Pitfield], à la page 12, au paragraphe 31.)

> [162] L'article 21 s'applique lorsque les méthodes traditionnelles sont insuffisantes pour faire progresser l'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 que cite le juge Noël s'appliquent à une technique envahissante en particulier.

[184] Dans *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] 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 [contacts] et ses habitudes de communication, [redacted] (ii) en tirant des conclusions sur [redacted] 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 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 [redacted] 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 [redacted] à l'égard de ces informations, par l'attente subjective en matière de vie privée qu'a probablement [redacted] 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 avec une autre, [redacted] 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 [redacted] 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 [redacted] 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 [redacted] 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 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, LRC (1985), ch C-23	*Canadian Security Intelligence Service Act*, RSC 1985, c C-23
Informations et renseignements	*Collection, analysis and retention*
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.	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.
Aucune limite territoriale	*No territorial limit*
(2) Il est entendu que le Service peut exercer les fonctions que le paragraphe (1) lui confère même à l'extérieur du Canada.	(2) For greater certainty, the Service may perform its duties and functions under subsection (1) within or outside 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 » (*Canada Trustco Mortgage Co v Canada*, 2005 CSC 54, 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] 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 *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)*, précité, 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 *Tessling*, précité, au paragraphe 30 et dans *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, au paragraphe 178 [*Mahjoub CAF*]). 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 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 « 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 » 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 RCS 495, aux pages 527 à 529 [*Simmons*] et *R. c Monney*, [1999] 1 RCS 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. (MR)*, [1998] 3 RCS 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 [redacted] 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 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 [redacted] 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 CFA*, 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 CFA*, 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 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 et 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 *X (Re)*, précité, 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 un juste équilibre entre l'intérêt public ayant trait aux enquêtes sur des menaces envers la sécurité du Canada et les droits de la cible en matière de vie privée quant aux activités qui ne sont que minimalement envahissantes (*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 RCS 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] 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 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 RCS 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, 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*, 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, 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 « les 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] 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 *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 [redacted] 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 [redacted] 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, 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 envahissante 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 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 concernant le caractère raisonnable de l'article 12

[236] Selon l'évaluation effectuée aux parties VII.C.3.(b)(i) à(iv), 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, 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 des ESB s'effectuent en général que le déroulement de l'opération ayant visé [redacted]

[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 [redacted] ont été détruites avant de faire l'objet de la moindre analyse et ne faisaient pas partie du rapport opérationnel préparé par le SCRS. [redacted] Dans la mesure où j'aborde différentes questions relatives à ces pouvoirs dans le dossier [redacted], 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, [redacted] a témoigné que le matériel du SCRS permet de garder le contact avec des appareils mobiles [redacted] [pendant quelques secondes]

[redacted] 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, [redacted] 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 [redacted] 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. [redacted] a témoigné que le SCRS a pour politique de ne pas recueillir un tel contenu.

[242] Enfin, selon [redacted] le SCRS élimine très rapidement les IMSI et les IMEI tirées d'appareils mobiles de tiers, souvent dans les [redacted] 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, [redacted] 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)-(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] 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 [redacted] 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 [redacted] constituait une fouille, car elle a aidé le SCRS à dresser un profil de [redacted] entre autres en lui permettant éventuellement d'esquisser ses [contacts] [redacted] 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 [redacted] 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, à une exception près [redacted] 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 [redacted] **[pendant quelques secondes]** [redacted] 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 [redacted] 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, [redacted] 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] 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 [redacted] 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] J'accorde aussi de l'importance à [redacted]

[256] J'ajouterai simplement trois autres conclusions.

[257] Premièrement, le SCRS ne doit pas s'appuyer sur le libellé du [redacted] 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] 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] 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).

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 [redacted] Cela ne contrevenait ni à la *Loi sur la radiocommunication Act*, LRC (1985), ch R-2, ni au *Code criminel*, LRC (1985), ch C-46, ni à l'article 8 de la *Charte canadienne des droits et libertés*, Partie I de la *Loi constitutionnelle de 1982*, annexe B de la *Loi de 1982 sur le Canada* (Royaume-Uni), ch 11. Même si l'utilisation d'un ESB contre [redacted] constituait une fouille, celle-ci n'était pas abusive, car elle était étroitement ciblée, très précise et minimalement envahissante.

Dans les sept (7) 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.

« Paul S. Crampton »

Le juge en chef

ANNEXE I

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.

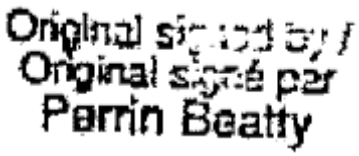
5) La présente autorisation n'écarte pas l'exigence d'obtenir la licence d'une station de radiocommunication ou l'autorisation exigée en vertu de la *Loi sur la radiocommunication* relativement aux appareils radio utilisés à des fins non prévues au paragraphe 2.

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.



Perrin Beatty
Ministre des Communications

Date : 1er sept. 1992

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* :

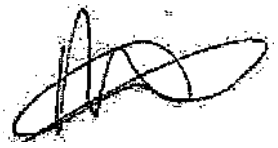
a) concernent les fonctions de composition, de routage, d'adressage ou de signalisation en matière de télécommunication;

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

ANNEXE III

***LOI SUR LE SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ*, LRC (1985), ch C-23**	***CANADIAN SECURITY INTELLIGENCE SERVICE ACT*, RSC 1985, c C-23**
Définitions	*Definitions*
2 Les définitions qui suivent s'appliquent à la présente loi.	2 In this Act,
menaces envers la sécurité du Canada	***threats to the security of Canada*** means
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;	(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) 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;	(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) 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;	(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) 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.	(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,
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).	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)

(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.

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

[…]

Management of Service

Role of Director

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

Minister may issue directions

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

Directions deemed not to be statutory instruments

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

Periodic reports by Director

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

Measures to reduce threats to the security of Canada

5) The reports shall include, among other things, the following information in respect of the Service's operational activities, during the

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 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.

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 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.

Assistance	*Collection of information concerning foreign states and persons*
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 :	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) d'un État étranger ou d'un groupe d'États étrangers;	(a) any foreign state or group of foreign states; or
b) d'une personne qui n'appartient à aucune des catégories suivantes :	(b) any person other than
(i) les citoyens canadiens,	(i) a Canadian citizen,
(ii) les résidents permanents au sens du paragraphe 2(1) de la *Loi sur l'immigration et la protection des réfugiés*,	(ii) a permanent resident within the meaning of subsection 2(1) of the *Immigration and Refugee Protection Act*, or
(iii) les personnes morales constituées sous le régime d'une loi fédérale ou provinciale.	(iii) a corporation incorporated by or under an Act of Parliament or of the legislature of a province.
Restriction	*Limitation*
(2) L'assistance autorisée au paragraphe (1) est subordonnée au fait qu'elle ne vise pas des personnes mentionnées à l'alinéa (1)b).	(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).
Consentement personnel des ministres	*Personal consent of Ministers required*
(3) L'exercice par le Service des fonctions visées au paragraphe (1) est subordonné :	(3) The Service shall not perform its duties and functions under subsection (1) unless it does so
a) à une demande personnelle écrite du ministre de la Défense nationale ou du ministre des Affaires étrangères;	(a) on the personal request in writing of the Minister of National Defence or the Minister of Foreign Affairs; and
b) au consentement personnel écrit du ministre.	(b) with the personal consent in writing of the Minister.
[…]	[…]

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

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

l’exercice, sont à autoriser ;

purpose;

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;

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

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

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

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

g) 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;

(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) 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.

(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.

Délivrance du mandat

Issuance of warrant

(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 :

(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) l’accès à un lieu ou un objet ou l’ouverture d’un objet;

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

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

(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,

l’établissement de copies ou d’extraits par tout procédé;

document or thing; or

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

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

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.

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.

Contenu du mandat

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

Matters to be specified in warrant

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

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;

(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;

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;

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

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

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

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

e) la durée de validité du mandat;

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

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

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

Durée maximale

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

Maximum duration of warrant

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

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.

(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.

Comité de surveillance des activités de renseignement de sécurité

Security Intelligence Review Committee

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.

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.

Durée du mandat

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

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.

Renouvellement

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

Re-appointment

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

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

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

séjour entraînés par l'exercice de ces fonctions.

by the member in the performance of those duties and functions.

[…]

[…]

Fonctions du comité de surveillance

Functions of Review Committee

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

38 (1) The functions of the Review Committee are

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

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

(i) [Abrogé, 2012, ch. 19, art. 381]

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

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

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

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

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

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

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

(vi) examiner les règlements,

(vi) to review the regulations, and

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

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

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

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

c) faire enquête sur :

(c) to conduct investigations in relation to

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

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

(ii) les rapports qui lui sont transmis en vertu

(ii) reports made to the Committee pursuant to section 19 of the *Citizenship Act*, and

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

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

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

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.

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.

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 :

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) 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);

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

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

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

[…]

[…]

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

***PRIVACY ACT*, RSC, 1985, c 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

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

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.

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.

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.

Special rules for hearings

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

(a) be heard in camera; and

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

***LOI SUR LA RADIOCOMMUNICATION*, LRC, ch R-2**

***RADIOCOMMUNICATION ACT*, RSC, 1985, c 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 :

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) délivrer et assortir de conditions :

(a) issue

(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) radio licences in respect of radio apparatus,

(i.1) les licences de spectre à l'égard de l'utilisation de fréquences de

(i.1) spectrum licences in respect of the utilization of specified radio frequencies within

radiocommunication définies dans une zone géographique déterminée, et notamment prévoir les conditions spécifiques relatives aux services pouvant être fournis par leur titulaire,

a defined geographic area,

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

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

(iii) les certificats d'opérateur radio,

(iii) radio operator certificates,

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

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

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

(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;

Interdictions

Prohibitions

9 (1) Il est interdit :

9 (1) No person shall

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;

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

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

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

(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) d'utiliser un appareil radio de façon à recevoir un signal d'abonnement ou une alimentation réseau ainsi décodé;

(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) de transmettre au public un signal d'abonnement ou une alimentation réseau ainsi

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

décodé.

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

Définitions

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

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

Interception

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

Réserve

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

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

b) 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

contravention of paragraph (c).

***CRIMINAL CODE*, RSC, 1985, c C-46**

Definitions

183 In this Part,

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

Interception

184 (1) Everyone 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 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

en conformité avec une telle autorisation ou en vertu de cet article;

authorization or pursuant to section 184.4;

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 :

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

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

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

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

(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;

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

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;

(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) 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 :

(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) 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,

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

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

Utilisation ou conservation

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

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

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

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).

Apparence de droit

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

Colour of right

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

COUR FÉDÉRALE

AVOCATS INSCRITS AU DOSSIER

DOSSIER :	[redacted]
INTITULÉ :	DANS L'AFFAIRE d'une demande de mandat présentée par [redacted] en vertu des articles 12 et 21 de la *Loi sur le service canadien du renseignement de sécurité*, LRC (1985), ch C-23 et DANS L'AFFAIRE VISANT le terrorisme islamiste et [redacted]
LIEU DE L'AUDIENCE :	OTTAWA (ONTARIO)
DATE DE L'AUDIENCE :	LE 17 MARS 2017 ET LE 4 MAI 2017
JUGEMENT ET MOTIFS :	LE JUGE EN CHEF CRAMPTON
DATE DES MOTIFS :	LE 22 AOÛT 2017

COMPARUTIONS

M[me] Jennifer Poirier M[me] Stéphanie Dion M[me] Ilana Bleichert	GROUPE LITIGES ET CONSEILS EN SÉCURITÉ NATIONALE DU MINISTÈRE DE LA JUSTICE
M. Gordon Cameron M. Owen Rees	*Amici Curiae*

AVOCATS INSCRITS AU DOSSIER

Procureure générale du Canada Ottawa (Ontario)	GROUPE LITIGES ET CONSEILS EN SÉCURITÉ NATIONALE DU MINISTÈRE DE LA JUSTICE
Blakes Cassels & Graydon LLP Ottawa (Ontario)	Avocats
Conway Baxter Wilson LLP Ottawa (Ontario)	