

[***]
2020 FC 697

[***]
2020 CF 697

In The Matter of an application by [*] for warrants pursuant to sections 16 and 21 of the *Canadian Security Intelligence Service Act*, R.S.C., 1985, c. C-23**

DANS L’AFFAIRE d’une demande de mandats présentée par [*] en vertu des articles 16 et 21 de la *Loi sur le service canadien du renseignement de sécurité*, L.R.C. (1985), ch. C-23**

And In The Matter of [*a foreign state, group of states, corporation or person***]**

Et dans l’affaire visant [*un État étranger, un groupe d’États étrangers, une personne morale étrangère ou une personne étrangère***]**

INDEXED AS: *CANADIAN SECURITY INTELLIGENCE SERVICE ACT (RE)*

RÉPERTORIÉ : *LOI SUR LE SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ (RE)*

Federal Court, O’Reilly J.—Ottawa, March 15, 16, 20, April 24, July 11, 2018 and June 16, 2020.

Cour fédérale, juge O’Reilly—Ottawa, 15, 16 et 20 mars, 24 avril, 11 juillet 2018 et 16 juin 2020.

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

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

*Security Intelligence — Application for warrants to gather foreign intelligence pursuant to Canadian Security Intelligence Service Act (CSIS Act or Act), s. 16 — Number of issues arising in context of s. 16 over recent years also considered — Act, s. 16 granting Canadian Security Intelligence Service (Service or CSIS) authority to provide assistance to Minister of National Defence or Minister of Foreign Affairs by collecting information or intelligence about capabilities, intentions, or activities of foreign state or foreign person — Service’s role under s. 16 distinct from its primary mandate to investigate threats to security of Canada under Act, s. 12 — Application including submissions on amendments that Service seeking to templates on which s. 16 warrants initially based, as well as representations on treatment of information collected about Canadians, including elected officials, during s. 16 investigations — Court appointing two amici curiae in proceeding; asked to address additional specific issues which consolidated — At issue was: scope of CSIS Act, s. 16 (particularly as it relates to collection of information about Canadians, to concurrent investigations of threats to security of Canada under s. 12, appropriate warrant templates for execution of intrusive powers in collection of foreign intelligence); whether s. 16 authorizing use of cellular site simulator (CSS) technology; whether s. 16 authorizing interception of [***] data; whether s. 16 authorizing interception of [***foreign persons***] communications outside Canada — Section 16 providing broad powers but Service’s mandate thereunder containing limits — Service’s authority to collect foreign intelligence strictly confined to foreign entities, precluding targeting of Canadians — Service can intercept communications of Canadians under s. 16 only incidentally;*

*Renseignement de sécurité — Demande de mandats visant la collecte de renseignements étrangers au titre de l’art. 16 de la Loi sur le service canadien du renseignement de sécurité (Loi sur le SCRS) — Un certain nombre de questions ayant trait à l’art. 16 soulevées au cours des dernières années ont été traitées également — L’art. 16 autorise le Service canadien du renseignement de sécurité (SCRS ou Service) à prêter son assistance au ministre de la Défense nationale ou au ministre des Affaires étrangères à la collecte d’informations ou de renseignements sur les moyens, les intentions ou les activités d’un étranger ou d’un État étranger — Ce rôle diffère de celui, fondamental, que l’art. 12 de cette même loi confie au Service : enquêter sur les menaces pour la sécurité du Canada — La demande était assortie d’observations portant sur des modifications que le Service voulait apporter aux modèles des mandats relatifs à l’art. 16, ainsi que sur le traitement des informations sur des Canadiens, y compris des élus, recueillies dans le cadre d’enquête menée au titre de ce même article — La Cour a nommé deux amici curiae et a été invitée à se prononcer sur d’autres points en particulier, qui avaient été rassemblés — Il s’agissait de savoir quelle est la portée de l’art. 16 de la Loi sur le SCRS (relativement, surtout, à la collecte d’informations sur des Canadiens, aux enquêtes menées simultanément sur les menaces pour la sécurité du Canada en vertu de l’art. 12 et aux modèles de mandats permettant l’exercice de pouvoirs intrusifs pour la collecte de renseignements étrangers); si l’art. 16 autorise le recours aux émulateurs de station de base (ESB); si l’art. 16 autorise l’interception de données [***]; et si l’art. 16 autorise l’interception de communications [***des personnes étrangères***] à l’extérieur*

has overarching duty to minimize intrusions on privacy of Canadians who are innocent third parties to s. 16 investigation — Where appropriate, Court can impose terms or conditions on execution of s. 16 warrant to curtail excessive intrusions on privacy — Parliamentary privilege not justifying creation of special rules or guidelines to address situations where communications of elected officials intercepted pursuant to s. 16 warrants — Service should advise Court of guidelines it develops for distributing, unminimizing identities of Canadians whose communications incidentally intercepted; permit Court opportunity to comment thereon — Service took steps to ensure no operational interaction existing between Service's foreign intelligence activities under s. 16, its s. 12 mandate relating to security intelligence; addressing Court's concerns in serious way — Service's proposed amendments would bring s. 16 warrant templates in line with s. 12 templates — Regarding Service's ability to capture information through use of CSS, minimally intrusive searches authorized by s. 16 without requirement of warrant — Sufficient safeguards constraining potential over-extension of Service's foreign intelligence role to satisfy Canadian Charter of Rights and Freedoms, s. 8 respecting minimally intrusive searches, such as use of CSS without warrant — Therefore, in present context, no significant difference between nature, purpose of s. 16 as compared to s. 12 — Interceptions of [***] data capture more personal information than CSS operations — Service engaging in [***] surveys whereby Service trying to identify particular device used by target of investigation — Surveys at issue may involve collection of intrusive lifestyle information — Thus, impartial judicial prior authorization (i.e. warrant) required for Service to collect such information — Act, s. 16 requiring that foreign intelligence be collected only "within Canada" which unambiguously meaning within Canada's geographical boundaries — Geographical requirements of s. 16 met when interceptions taking place within Canada in respect of communications outside Canada — Application allowed.

This case began as an application for warrants to gather foreign intelligence pursuant to section 16 of the *Canadian*

du Canada — L'art. 16 accorde des pouvoirs étendus, mais le rôle qu'il confère au Service est limité — Le pouvoir de ce dernier de recueillir des renseignements étrangers est strictement circonscrit aux entités étrangères; il ne peut pas viser des Canadiens — Le Service ne peut intercepter les communications de Canadiens au titre de l'art. 16 que de manière incidente; il est tenu de minimiser le degré d'empiètement sur la vie privée de Canadiens qui sont des tiers innocents dans le cadre d'une enquête menée au titre de l'art. 16 — S'il y a lieu, la Cour peut imposer des conditions à l'exécution d'un mandat relatif à l'art. 16 afin de limiter l'empiètement excessif sur la vie privée — Le privilège parlementaire ne justifie pas la création de règles ou de directives spéciales pour le traitement des cas d'interception de communications d'élus au titre de l'art. 16 — Le Service devrait informer la Cour de la teneur des lignes directrices qu'il se donne quant au renversement de la divulgation minimale d'informations permettant de reconnaître des Canadiens dont les communications ont été interceptées de manière incidente, et donner à la Cour l'occasion de les commenter — Le Service a pris des mesures pour qu'il n'y ait aucune interaction de nature opérationnelle entre les activités de renseignement étranger qu'il mène en lien avec l'art. 16 et le mandat que lui donne l'art. 12 en matière de renseignement de sécurité; il a tenu compte des préoccupations de la Cour avec sérieux — Le Service a proposé des modifications destinées à aligner les modèles de mandats liés à l'art. 16 sur ceux liés à l'art. 12 — En ce qui concerne la capacité du Service de capturer des informations au moyen d'ESB, l'art. 16 autorise la réalisation, sans mandat, de fouilles minimalement envahissantes — Il existe suffisamment de mécanismes permettant d'empêcher le Service d'aller trop loin dans son rôle eu égard au renseignement étranger pour que soit respecté l'art. 8 de la Charte canadienne des droits et libertés quant aux fouilles minimalement envahissantes menées sans mandat, comme l'utilisation d'ESB — Partant, dans ce contexte, il n'y avait aucune différence importante entre les art. 12 et 16 en ce qui a trait à la nature et à l'objet — L'interception de données [***] permet d'obtenir davantage d'informations personnelles que les opérations fondées sur les ESB — Le Service effectue des sondages [***] par lesquels il tente de reconnaître l'appareil en particulier qu'utilise la cible de l'enquête — Les sondages en question peuvent entraîner la collecte envahissante d'informations sur le mode de vie — Par conséquent, le Service doit obtenir au préalable une autorisation judiciaire impartiale, c'est-à-dire un mandat, pour recueillir ces informations — Aux termes de l'art. 16, les renseignements étrangers ne peuvent être recueillis que « dans les limites du Canada », ce qui signifie, sans équivoque, dans les frontières géographiques du pays — Il y a respect de la restriction géographique de l'art. 16 lorsqu'il y a interception, dans les limites du Canada, de communications à l'étranger — Demande accueillie.

Une demande de mandats visant la collecte de renseignements étrangers au titre de l'article 16 de la *Loi sur le service*

Security Intelligence Service Act (CSIS Act or Act). It then grew, becoming a vehicle for the consideration of a number of issues that have arisen in the context of section 16 over recent years. Section 16 of the Act grants the Canadian Security Intelligence Service (Service or CSIS) authority to provide assistance to the Minister of National Defence or the Minister of Foreign Affairs by collecting information or intelligence about the capabilities, intentions, or activities of a foreign state or foreign person. The Service's role under section 16 is distinct from its primary mandate to investigate threats to the security of Canada under section 12 of the Act. When the original application was heard, the Court was alerted that the application would include submissions on amendments that the Service was seeking to the templates on which section 16 warrants were then based, as well as representations on the treatment of information collected about Canadians, including elected officials, in the course of section 16 investigations. The latter was in response to an earlier Direction from the Court requesting the Service to explain its practices and procedure in a future section 16 warrant application. Two *amici curiae* were appointed by the Court. Later, the Attorney General of Canada (AGC) sought to address other issues that had not been previously considered by the Court in the section 16 context. In addition to the issues relating to the warrant templates and the treatment of information about Canadians, the AGC, jointly with the *amici*, requested that the Court address other specific issues. These various issues were consolidated and rulings were made.

At issue was: the scope of section 16 of the CSIS Act (particularly as it relates to the collection of information about Canadians and to concurrent investigations of threats to the security of Canada under section 12, and the appropriate warrant templates for the execution of intrusive powers in the collection of foreign intelligence); whether section 16 authorizes use of cellular site simulator (CSS) technology; whether section 16 authorizes interception of [***] data; and whether section 16 authorizes interception of [***foreign persons***] communications outside Canada.

Held, the application should be allowed.

Although the Service's need to be involved in protecting Canada from foreign clandestine activities is merely a secondary role, section 16 provides broad powers. However, the Service's section 16 mandate contains limits. Its authority to collect foreign intelligence has always been strictly confined to foreign entities and has precluded the targeting of Canadians. Section 16 allows the Service, within Canada, to gather information or intelligence about a foreign state or group of foreign states, or of a person who is not a Canadian citizen, permanent

canadien du renseignement de sécurité (Loi sur le SCRS) était à l'origine de la présente espèce, qui a ensuite pris de l'ampleur pour devenir un véhicule propice au traitement de questions ayant trait à l'article 16 soulevées au cours des dernières années. L'article 16 de la Loi sur le SCRS autorise le Service canadien du renseignement de sécurité (SCRS ou Service) à prêter son assistance au ministre de la Défense nationale ou au ministre des Affaires étrangères à la collecte d'informations ou de renseignements sur les moyens, les intentions ou les activités d'un étranger ou d'un État étranger. Ce rôle diffère de celui, fondamental, que l'article 12 de cette même loi confie au Service : enquêter sur les menaces pour la sécurité du Canada. Lors de l'audition de la demande originale, la Cour a été avisée que la demande serait assortie d'observations portant sur des modifications que le Service voulait apporter aux modèles des mandats relatifs à l'article 16, ainsi que sur le traitement des informations sur des Canadiens, y compris des élus, recueillies dans le cadre d'enquête menée au titre de ce même article. Ce dernier point faisait suite à une directive antérieure par laquelle la Cour avait demandé au Service d'expliquer ses pratiques et procédures dans une future demande de mandats relatifs à l'article 16. La Cour a nommé deux *amici curiae*. Par la suite, le procureur général du Canada (procureur général) a cherché à aborder des questions que la Cour n'avait pas encore prises en considération dans le contexte de l'article 16. Outre ce qui concernait les modèles de mandats et le traitement des informations sur des Canadiens, le procureur général, d'un commun accord avec les *amici*, a demandé que la Cour se prononce sur d'autres points en particulier. Ces diverses questions ont été rassemblées et des décisions ont été rendues.

Il s'agissait de savoir quelle est la portée de l'article 16 de la Loi sur le SCRS (relativement, surtout, à la collecte d'informations sur des Canadiens, aux enquêtes menées simultanément sur les menaces pour la sécurité du Canada en vertu de l'article 12 et aux modèles de mandats permettant l'exercice de pouvoirs intrusifs pour la collecte de renseignements étrangers); si l'article 16 autorise le recours aux émulateurs de station de base (ESB); si l'article 16 autorise l'interception de données [***]; et si l'article 16 autorise l'interception de communications [***des personnes étrangères***] à l'extérieur du Canada.

Jugement : la demande doit être accueillie.

Bien que la participation du Service à la protection du Canada contre les activités clandestines d'origine étrangère ne soit qu'un rôle secondaire, l'article 16 accorde des pouvoirs étendus. Par contre, le rôle que confère l'article 16 au Service est limité. Son pouvoir de recueillir des renseignements étrangers a toujours été strictement circonscrit aux entités étrangères; il ne peut pas viser des Canadiens. L'article 16 autorise le Service, dans les limites du Canada, à recueillir des informations ou des renseignements sur un État étranger ou

resident of Canada, or a Canadian corporation. This means that the Service can intercept communications of Canadians under section 16 only incidentally. The Service has an overarching duty to minimize intrusions on the privacy of Canadians who are innocent third parties to a section 16 investigation. Where appropriate, the Court can impose terms or conditions on the execution of a section 16 warrant to curtail excessive intrusions on privacy. The fact that incidental collection of communications by, and information about, Canadians is an inevitable by-product of the collection of foreign intelligence under section 16 has been recognized since the creation of the Service. At the same time, the collection, retention, and use of incidentally intercepted information raises concerns about Canadians' privacy. Previously, the Court had requested an explanation from the Service as to CSIS retention practices of communications of Canadians with [***foreign person***] in particular. On receiving the Service's response, a further Direction was issued directing that the legal issue on the legitimacy of collection and retention when related to information on Canadians, and even more so when such Canadians are democratically elected representatives, be raised as part of a new section 16 warrant application to allow the Court to have all the information needed to make a proper determination if required. The Service complied with this Direction in the present application. Regarding the Service's practices relating to information about Canadians, the Service emphasized the scope of the current safeguards in respect of the collection of foreign intelligence pursuant to section 16. A policy on the minimization of information about Canadians was also adopted and this serves to limit disclosure of the identities of Canadians in all section 16 related intelligence.

A particular concern related to the incidental interception of communications between members of federal or provincial legislatures and foreign persons or entities—an inevitable consequence of foreign intelligence gathering. Parliamentary privilege does not justify the creation of special rules or guidelines to address situations where the communications of elected officials are intercepted pursuant to section 16 warrants. The *amici* were right in stating that the Service should develop criteria and guidelines on the unminimization of identifying information about Canadians. Greater protection should be granted to information about Canadians incidentally collected in the gathering of foreign intelligence. Without guidelines, decisions about the retention, disclosure, and distribution of this information is left to individual discretion. The information about Canadians that the Service obtains in this fashion merits special care and respect. That is even more true for

un groupe d'États étrangers, ou sur une personne qui n'est pas un citoyen canadien, un résident permanent du Canada ou une personne morale constituée au Canada. Partant, le Service ne peut intercepter les communications de Canadiens au titre de l'article 16 que de manière incidente. Le Service est tenu de minimiser le degré d'empiètement sur la vie privée de Canadiens qui sont des tiers innocents dans le cadre d'une enquête menée au titre de l'article 16. S'il y a lieu, la Cour peut imposer des conditions à l'exécution d'un mandat relatif à l'article 16 afin de limiter l'empiètement excessif sur la vie privée. Le caractère inévitable de l'interception de communications de Canadiens et de l'obtention d'informations sur des Canadiens de manière incidente dans le cadre de la collecte de renseignements étrangers au titre de l'article 16 est un état de fait reconnu depuis la création du Service. Parallèlement, la collecte, la conservation et l'utilisation des informations recueillies de manière incidente soulèvent des préoccupations quant à la vie privée des Canadiens. Par le passé, la Cour a demandé au Service de fournir des explications sur ses [TRADUCTION] « pratiques de conservation de communications de Canadiens avec [***des personnes étrangères***] » en particulier. Par suite de la réponse du Service, la Cour a formulé une autre directive dans laquelle elle a demandé que la question juridique de la légitimité de la collecte et de la conservation d'informations sur des Canadiens, surtout lorsqu'il s'agit de représentants élus démocratiquement, soit soulevée dans une nouvelle demande de mandats relatifs à l'article 16 afin que la Cour puisse avoir à sa disposition toutes les informations nécessaires pour se prononcer adéquatement, s'il y a lieu. Le Service s'est conformé à cette directive dans la demande en l'espèce. En ce qui concerne les pratiques du Service quant aux informations sur des Canadiens, le Service a mis en relief la portée des mesures de protection en vigueur quant à la collecte de renseignements étrangers au titre de l'article 16. Une politique sur la divulgation minimale d'informations sur des Canadiens a été adoptée également, et elle sert à limiter la divulgation de l'identité de Canadiens dans tout renseignement lié à l'article 16.

L'interception, de manière incidente, de communications entre des députés fédéraux ou provinciaux et des étrangers ou des organisations étrangères a soulevé une préoccupation particulière, mais il s'agit d'une conséquence inévitable de la collecte de renseignements étrangers. Le privilège parlementaire ne justifie pas la création de règles ou de directives spéciales pour le traitement des cas d'interception de communications d'élus au titre de l'article 16. Les *amici* ont déclaré à juste titre que le Service devrait se donner des critères et des lignes directrices quant au renversement de la divulgation minimale d'informations permettant de reconnaître des Canadiens. Il y a lieu d'accroître la protection accordée aux informations sur des Canadiens recueillies de manière incidente dans le cadre de la collecte de renseignements étrangers. Sans lignes directrices, les décisions sur la conservation, la communication et la diffusion de ces informations relèvent de

information about public officials and senior public officials, as the Service's policies already recognize. The Service should advise the Court of the content of the guidelines on this matter it develops and permit the Court an opportunity to comment on them. In individual warrant applications, the Service should continue to inform the Court when there may be incidental interceptions of Canadians' communications. It should also specifically disclose when there is a possibility that the communications of an elected official or other public servant may be intercepted. This disclosure requirement will permit the Court, where appropriate, to attach terms and conditions on the execution of the warrants it issues.

An ongoing concern was the potential overlap between, or the blending of, the Service's mandates under section 16 and section 12 of the Act. Accordingly, the Service was asked to address this issue based on the observation that some recent requests for warrants under section 16 for foreign intelligence purposes resemble applications under section 12 for warrants to investigate threats to national security. The concern was that section 16 could come to be used as an alternative or a supplement to section 12 contrary to the intention of Parliament when enacting the CSIS Act. The Service satisfactorily addressed this issue. The evidence they submitted showed that the Service has taken steps to ensure that there is no operational interaction between the Service's foreign intelligence activities under section 16 and its section 12 mandate relating to security intelligence. In brief, the Service addressed all concerns in a serious way in both its operations and policies and there was no need to propose any further action on the Service's part.

The Service proposed a number of amendments that would bring section 16 warrant templates in line with section 12 templates. The proposed modifications did not raise any legal issues. Any changes or improvements to the wording of the section 12 warrant templates should generally result in corresponding changes to the warrant templates applicable in the foreign intelligence context.

The Service sought to confirm that its authority pursuant to section 16 of the CSIS Act includes the ability to capture information through use of CSS, which can be used to obtain data emitted by mobile devices. Minimally intrusive searches are authorized by section 16 without the requirement of a warrant. There are at least three notable differences in the nature and purpose of section 16 as compared to section 12. First, the role given to the Service under section 16 is permissive, not mandatory. Second, the Service's section 16 mandate is not a direct responsibility to collect intelligence. The Service's role

la discrétion de chacun. Les informations sur des Canadiens que le Service obtient ainsi méritent d'être traitées avec un soin particulier, à plus forte raison celles qui touchent des représentants officiels et de hauts fonctionnaires, comme le reconnaissent déjà les politiques du Service. Le Service devrait informer la Cour de la teneur de ces lignes directrices et lui donner l'occasion de les commenter. Dans chaque demande de mandats, le Service devrait continuer d'informer la Cour des cas possibles d'interception, de manière incidente, de communications de Canadiens, particulièrement s'il peut s'agir d'élus ou de fonctionnaires. Au besoin, la Cour pourra ainsi fixer des conditions à l'exécution des mandats qu'elle décerne.

Le possible chevauchement des rôles confiés au Service par les articles 12 et 16 de la Loi sur le SCRS, voire la confusion entre les deux, constituait une préoccupation permanente. Partant, le Service a été prié d'étudier la question, compte tenu du fait que certaines demandes de mandats récemment faites au titre de l'article 16 en matière de renseignement étranger ressemblaient à des demandes de mandats relatives à des enquêtes sur des menaces pour la sécurité nationale, qui relèvent de l'article 12. Cette situation était préoccupante en ce sens que l'article 16 pourrait finir par servir de solution de rechange ou de complément à l'article 12, contrairement à l'intention du législateur à l'adoption de la Loi sur le SCRS. Le Service a réglé cette question de façon satisfaisante. La preuve qu'il a produite a démontré qu'il a pris des mesures pour qu'il n'y ait aucune interaction de nature opérationnelle entre les activités de renseignement étranger qu'il mène en lien avec l'article 16 et le mandat que lui donne l'article 12 en matière de renseignement de sécurité. Bref, le Service a tenu compte de toutes les préoccupations avec sérieux tant dans ses opérations que dans ses politiques, et il n'était pas nécessaire de proposer l'adoption d'autres mesures par le Service.

Le Service a proposé un certain nombre de modifications destinées à aligner les modèles de mandats liés à l'article 16 sur ceux liés à l'article 12. Ces modifications ne soulevaient aucune question juridique. En règle générale, tout changement ou toute amélioration au libellé des modèles de mandats relatifs à l'article 12 devrait entraîner des modifications correspondantes dans les modèles de mandats applicables au renseignement étranger.

Le Service a cherché à confirmer que ses pouvoirs au titre de l'article 16 de la Loi sur le SCRS comprennent la capacité de capturer des informations au moyen d'émutateurs de station de base (ESB), qui peuvent permettre d'obtenir des données émises par des appareils mobiles. L'article 16 autorise la réalisation, sans mandat, de fouilles minimalement envahissantes. Il existe au moins trois grandes différences entre la nature et l'objet des articles 12 et 16. D'abord, l'article 16 donne au Service une autorisation; il ne lui impose pas une contrainte. Ensuite, l'article 16 ne charge pas directement le Service de recueillir

is to assist the named ministers. Third, section 16 does not require that the collection of the information or intelligence be “strictly necessary” or set out a standard comparable to the “reasonable suspicion” threshold. While the mandate given to the Service under section 16 differs in important ways from its section 12 role, that is not the equivalent of stating that the nature and purpose of section 16 is somehow less important or less vital to Canada’s interests than those animating section 12. There exists sufficient safeguards constraining the potential over-extension of the Service’s foreign intelligence role to satisfy section 8 of the *Canadian Charter of Rights and Freedoms* in respect of minimally intrusive searches, such as the use of CSS, without a warrant. Therefore, in this context, there was not a significant difference between the nature and purpose of section 16 as compared to section 12. In both areas, the Service’s role furthers pressing national interests. In addition, though section 16 may lack the limiting language of section 12, it contains an essential constraint that does not apply to section 12—section 16 targets only foreign persons and states, not Canadians. Therefore, no conflict between the warrantless use of CSS and section 8 of the Charter existed. Section 16 provides a sufficient and reasonable statutory basis for warrantless searches, so long as they are minimally intrusive and conducted in a reasonable manner.

Interceptions of [***] data capture more personal information than CSS operations and require a warrant. The Service engages in [***] surveys, whereby the Service obtains [***] in an effort to identify a particular device used by a target of an investigation. A survey involves the use of a device specially configured to capture [***]. The Service submitted that the most valuable information it obtains in support of its section 16 mandate often comes from intercepted communications of those [***foreign persons***] who are associated with [***foreign states, groups of foreign states, or foreign corporations***] in respect of which the Service is currently assisting the Minister. Similar to the use of CSS technology, the surveys at issue allow the Service to obtain the unique electronic identifiers associated with the devices which, in turn, will permit the Service to conduct warranted interceptions. Minimally intrusive [***] surveys conducted pursuant to section 16 are carried out reasonably. As with CSS technology, there is no impact on any private communications or other private information stored in the device. Any third-party information collected is destroyed. Given the difference between CSS operations, which involve minimally intrusive collections, and the surveys at issue, which may involve collection of intrusive lifestyle information, the latter require a warrant. These surveys may result in the gathering of personal information that is not open to public view and not released or abandoned by the targets of investigations. These factors tend in the direction of requiring a

des renseignements. Le rôle du Service est de prêter son assistance aux ministres mentionnés. Enfin, l’article 16 n’exige pas que la collecte d’informations ou de renseignement se fasse « dans la mesure strictement nécessaire » ni n’établit un critère comparable à celui des « motifs raisonnables de soupçonner ». S’il existe des différences importantes entre les rôles que confèrent au Service les articles 12 et 16, cela ne revient pas à affirmer que la nature et l’objet de l’article 16 sont, en quelque sorte, moins importants ou cruciaux pour les intérêts du Canada que ceux de l’article 12. Il existe suffisamment de mécanismes permettant d’empêcher le Service d’aller trop loin dans son rôle eu égard au renseignement étranger pour que soit respecté l’article 8 de la *Charte canadienne des droits et libertés* quant aux fouilles minimalement envahissantes menées sans mandat, comme l’utilisation d’ESB. Partant, dans ce contexte, il n’y avait aucune différence importante entre les articles 12 et 16 en ce qui a trait à la nature et à l’objet. Dans les deux domaines, le rôle du Service sert les intérêts nationaux. En outre, bien qu’il ne comporte pas le libellé limitatif de l’article 12, l’article 16 comporte une contrainte essentielle à laquelle échappe l’article 12 : seuls des étrangers et des États étrangers peuvent être visés; les cibles ne peuvent pas être des Canadiens. Partant, il n’existe aucun conflit entre l’utilisation d’ESB sans mandat et l’article 8 de la Charte. L’article 16 offre un fondement légal suffisant et raisonnable aux fouilles sans mandat, pourvu qu’elles soient minimalement envahissantes et effectuées de manière raisonnable.

L’interception de données [***] permet d’obtenir davantage d’informations personnelles que les opérations fondées sur les ESB et nécessite un mandat. Le Service effectue ce qu’il appelle des « sondages [***] » qui lui permettent d’obtenir [***] en vue de reconnaître celui qu’utilise la cible de l’enquête. Pour ce faire, il utilise un appareil spécialement configuré pour capter [***]. Le Service a avancé que les informations les plus utiles qu’il recueille dans l’exercice du rôle que lui confie l’article 16 découlent des communications interceptées [***des personnes étrangères***] qui sont associées à [***des États étrangers, groupes d’États étrangers, ou personnes morales étrangères***] à propos desquels il prête actuellement son assistance au ministre. À l’instar des ESB, les sondages en question permettent au Service d’obtenir les identifiants électroniques uniques ayant trait aux appareils, ce qui lui permet ensuite de procéder, en vertu de mandats, à des interceptions. Les sondages [***] minimalement envahissants, menés au titre de l’article 16, le sont raisonnablement. Comme pour la technologie relative aux ESB, il n’y a aucune incidence sur les communications privées ou toute autre information privée stockée dans l’appareil. Les informations de tiers recueillies sont détruites. Compte tenu de la différence entre une opération fondée sur les ESB, qui implique une collecte minimalement envahissante, et les sondages en question, qui peuvent entraîner la collecte envahissante d’informations sur le mode de vie, ce dernier nécessite un mandat. De tels sondages peuvent

warrant. While section 16 is a reasonable law to the extent that it permits conducting minimally intrusive searches without a warrant, the same conclusion could not be reached regarding the surveys at issue that collect personal lifestyle information. Thus, impartial judicial prior authorization—a warrant—is required for the Service to collect that information.

Section 16 requires that foreign intelligence be collected only “within Canada”. The words “within Canada” have been the subject of other litigation in the Court, most particularly in the case of *X (Re)* ([**]) where it was concluded that the words “within Canada” in section 16 unambiguously mean within Canada’s geographical boundaries. The geographical requirements of section 16 are met when interceptions take place within Canada in respect of communications outside Canada. In the absence of clear legal authority permitting the Service to intercept a person’s communications outside of Canada, the Service’s current practice is to terminate an interception if it becomes aware that a subject has left Canada. However, if the Service is not aware of that, the interceptions will continue. Based on the evidence, the Service’s proposed interceptions will be made within Canada and will comply with the geographical limits of section 16.

STATUTES AND REGULATIONS CITED

Canadian Charter of Rights and Freedoms, being Part I of the *Constitution Act, 1982*, Schedule B, *Canada Act 1982*, 1982, c. 11 (U.K.) [R.S.C., 1985, Appendix II, No. 44], s. 8.
Canadian Security Intelligence Service Act, R.S.C., 1985, c. C-23, ss. 2 “threats to the security of Canada”, 12, 12.1, 12.2, 16, 21, 21.1.
Criminal Code, R.S.C., 1985, c. C-46, ss. 184, 430(1.1)(c).
Radiocommunication Act, R.S.C., 1985, c. R-2, s. 9(1)(b).

CASES CITED

APPLIED:

X (Re), 2018 FC 738, [2019] 1 F.C.R. 567, aff’d 2018 FCA 207; *Canada (House of Commons) v. Vaid*, 2005 SCC 30, [2005] 1 S.C.R. 667; *X (Re)*, 2017 FC 1047, [2018] 3 F.C.R. 111.

mener à la collecte de renseignements personnels à caractère privé, qui n’ont été ni divulgués ni abandonnés par la cible d’une enquête. Ces facteurs tendent à démontrer qu’un mandat est nécessaire. Si l’article 16 est une disposition législative raisonnable qui permet la réalisation de fouilles minimalement envahissantes sans mandat, il est impossible de trancher de la même manière en ce qui a trait aux sondages en question qui permettent de recueillir des renseignements personnels sur le mode de vie. Par conséquent, le Service doit obtenir au préalable une autorisation judiciaire impartiale, c’est-à-dire un mandat, pour recueillir ces informations.

Aux termes de l’article 16, les renseignements étrangers ne peuvent être recueillis que « dans les limites du Canada ». La Cour a été saisie d’autres litiges relatifs à l’expression « dans les limites du Canada », surtout dans *X (Re)* ([**]), où elle a conclu que l’expression « dans les limites du Canada » figurant à l’article 16 signifie, sans équivoque, dans les frontières géographiques du pays. Il y a respect de la restriction géographique de l’article 16 lorsqu’il y a interception, dans les limites du Canada, de communications à l’étranger. Puisqu’aucune disposition législative ne l’autorise clairement à intercepter les communications d’une personne à l’étranger, le Service a pour pratique de mettre fin à l’interception s’il apprend que [la personne étrangère] a quitté le Canada. L’interception se poursuivra cependant si [**] la personne étrangère [**] quitte le pays à l’insu du Service. Compte tenu de ces éléments de preuve, les interceptions que propose le Service auront lieu dans les limites du Canada et, partant, respecteront la restriction géographique prévue à l’article 16.

LOIS ET RÈGLEMENTS CITÉS

Charte canadienne des droits et libertés, qui constitue la partie I de la *Loi constitutionnelle de 1982*, annexe B, *Loi de 1982 sur le Canada*, 1982, ch. 11 (R.-U.) [L.R.C. (1985), appendice II, n° 44], art. 8.
Code criminel, L.R.C. (1985), ch. C-46, art. 184, 430(1.1)c).
Loi sur la radiocommunication, L.R.C. (1985), ch. R-2, art. 9(1)b).
Loi sur le Service canadien du renseignement de sécurité, L.R.C. (1985), ch. C-23, art. 2 « menaces envers la sécurité du Canada », 12, 12.1, 12.2, 16, 21, 21.1.

JURISPRUDENCE CITÉE

DÉCISIONS APPLIQUÉES :

X (Re), 2018 CF 738, [2019] 1 R.C.F. 567, conf. par. 2018 CAF 207; *Canada (Chambre des communes) c. Vaid*, 2005 CSC 30, [2005] 1 R.C.S. 667; *X (Re)*, 2017 CF 1047, [2018] 3 R.C.F. 111

CONSIDERED:

X (Re), 2016 FC 1105, [2017] 2 F.C.R. 396; *Canadian Security Intelligence Service Act (Re)*, 2012 FC 1437, [2014] 2 F.C.R. 514; *Caroline Lucas MP and Ors v. Security Service and Ors*, [2015] UKIPTrib 14_79-CH; *R. v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212; *X (Re)*, 2009 FC 1058, [2010] 1 F.C.R. 460.

REFERRED TO:

R. v. Chesson, [1988] 2 S.C.R. 148, (1988), 90 A.R. 347; *Pankiw v. Canada (Human Rights Commission)*, 2006 FC 1544, [2007] 4 F.C.R. 578; *R. v. Shoker*, 2006 SCC 44, [2006] 2 S.C.R. 399; *R. v. Nova Scotia Pharmaceutical Society*, [1992] 2 S.C.R. 606, (1992), 93 D.L.R. (4th) 36; *R. v. Chehil*, 2013 SCC 49, [2013] 3 S.C.R. 220; *R. v. Collins*, [1987] 1 S.C.R. 265, (1987), 38 D.L.R. (4th) 508; *R. v. A.M.*, 2008 SCC 19, [2008] 1 S.C.R. 569; *R. v. Reeves*, 2018 SCC 56, [2018] 3 S.C.R. 531; *R. v. Marakah*, 2017 SCC 59, [2017] 2 S.C.R. 608; *R. v. Kang-Brown*, 2008 SCC 18, [2018] 1 S.C.R. 456; *R. v. Plant*, [1993] 3 S.C.R. 281, (1993), 145 A.R. 104; *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432.

AUTHORS CITED

British Columbia. Legislative Assembly, *Hansard*, 32nd Parl., 2nd Sess. (June 6, 1980).

Canada. Parliament. House of Commons. Standing Committee on Justice and Legal Affairs. *Minutes of Proceedings and Evidence*, 32nd Parl., 2nd Sess., Issue No. 38 (June 7, 1984).

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

Canada. Parliament. Senate. Special Committee of the Senate on the Canadian Security Intelligence Service, *Proceedings of the Senate on the Canadian Security Intelligence Service on the subject matter of Bill C-157*, 32nd Parl., 1st Sess., 1983.

Canada. Public Safety. *Ministerial Directive on Legislators' Privileges and Immunities in relation to Part IV.1 of the Criminal Code within the Precincts of Parliament, Provincial and Territorial Assemblies*, Ottawa: Solicitor General Canada, 1983.

Cheifetz, David. "Protection of Confidential Communications of Members of Parliament" (1981), 4 *Can. Parl. Rev.* 17.

House of Commons Procedure and Practice, 2nd ed. Ottawa: House of Commons, 2009.

Security Intelligence Review Committee. *Annual Report*, 1993–1994.

DÉCISIONS EXAMINÉES :

X (Re), 2016 CF 1105, [2017] 2 R.C.F. 396; *Renvoi relatif à la Loi sur le Service canadien du renseignement de sécurité*, 2012 CF 1437, [2014] 2 R.C.F. 514; *Caroline Lucas MP and Ors v. Security Service and Ors*, [2015] UKIPTrib 14_79-CH; *R. c. Spencer*, 2014 CSC 43, [2014] 2 R.C.S. 212; *X (Re)*, 2009 CF 1058, [2010] 1 R.C.F. 460

DÉCISIONS CITÉES :

R. c. Chesson, [1988] 2 R.C.S. 148; *Pankiw c. Canada (Commission des droits de la personne)*, 2006 CF 1544, [2007] 4 R.C.F. 578; *R. c. Shoker*, 2006 CSC 44, [2006] 2 R.C.S. 399; *R. c. Nova Scotia Pharmaceutical Society*, [1992] 2 S.C.R. 606; *R. c. Chehil*, 2013 CSC 49, [2013] 3 R.C.S. 220; *R. c. Collins*, [1987] 1 R.C.S. 265; *R. c. A.M.*, 2008 CSC 19, [2008] 1 R.C.S. 569; *R. c. Reeves*, 2018 CSC 56, [2018] 3 R.C.S. 531; *R. c. Marakah*, 2017 CSC 59, [2017] 2 R.C.S. 608; *R. c. Kang-Brown*, 2008 CSC 18, [2018] 1 R.C.S. 456; *R. c. Plant*, [1993] 3 R.C.S. 281; *R. c. Tessling*, 2004 CSC 67, [2004] 3 R.C.S. 432.

DOCTRINE CITÉE

Canada. Parlement. Chambre des communes. Comité permanent de la Justice et des questions juridiques, *Procès-verbaux et témoignages*, 32^e lég., 2^e sess., fascicule n^o 38 (7 juin 1984).

Canada. Parlement. Sénat. Comité sénatorial spécial sur le Service canadien du renseignement de sécurité, *Délibérations du comité sénatorial spécial du Service canadien du renseignement de sécurité sur la teneur du projet de loi C-157*, 32^e lég., 1^{re} sess., 1983.

Canada. Parlement. Sénat. Rapport du comité sénatorial spécial sur le Service canadien du renseignement de sécurité. *Équilibre délicat : Un service du renseignement de sécurité dans une société démocratique*. Ottawa : Approvisionnements et Services Canada, novembre 1983.

Canada. Sécurité publique. *Ministerial Directive on Legislators' Privileges and Immunities in relation to Part IV.1 of the Criminal Code within the Precincts of Parliament, Provincial and Territorial Assemblies*, Ottawa : Solliciteur général Canada, 1983.

Cheifetz, David. « La protection accordée aux communications des députés » (1981), 4 *Rev. parl. can.* 17.

Colombie-Britannique. Legislative Assembly, *Hansard*, 32^e lég., 2^e sess. (6 juin 1980).

Comité de surveillance des activités de renseignement de sécurité. *Rapport annuel*, 1993–1994.

Taylor, Donald E. “Electronic Surveillance and Members’ Privileges” (1989), 12 *Can. Parl. Rev.* 12.

La procédure et les usages de la Chambre des communes, 2^e éd. Ottawa : Chambre des communes, 2009.

Taylor, Donald E. « La surveillance électronique et l’immunité parlementaire » (1989), 12 *Rev. parl. can.* 12.

APPLICATION for warrants to gather foreign intelligence pursuant to section 16 of the *Canadian Security Intelligence Service Act* whereby the initial application grew to consider a number of issues that arose in the context of section 16 of the Act over recent years. Application allowed.

DEMANDE de mandats visant la collecte de renseignements étrangers au titre de l’article 16 de la *Loi sur le service canadien du renseignement de sécurité* à l’origine de la présente espèce, qui a ensuite pris de l’ampleur pour traiter des questions ayant trait à l’article 16 soulevées au cours des dernières années. Demande accueillie.

APPEARANCES

Jennifer Poirier and *Amy Joslin-Besner* for applicant Attorney General of Canada.
Gordon Cameron and *Owen Rees* as *amici curiae*.

ONT COMPARU :

Jennifer Poirier et *Amy Joslin-Besner* pour le demandeur, le procureur général du Canada.
Gordon Cameron et *Owen Rees* à titre d’*amici curiae*.

SOLICITORS OF RECORD

Deputy Attorney General of Canada for applicant Attorney General of Canada.
Gordon Cameron and *Owen Rees* as *amici curiae*.

AVOCATS INSCRITS AU DOSSIER

Le sous-procureur général du Canada pour le demandeur, le procureur général du Canada.
Gordon Cameron et *Owen Rees* à titre d’*amici curiae*.

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

Ce qui suit est la version française des motifs du jugement et du jugement rendu par

O’REILLY J.:

LE JUGE O’REILLY :

Table of Contents

Table des matières

	Paragraph
I. Background.....	1
II. Issue One—What is the scope of section 16 of the CSIS Act?	10
A. Background—The History and Purpose of section 16.....	11
B. Incidental Collection of Information About Canadians.....	18
(1) Introduction.....	18
(2) Background.....	21

	Paragraphe
I. Contexte	1
II. Première question — Quelle est la portée de l’article 16 de la Loi sur le SCRS?	10
A. Contexte — Historique et objet de l’article 16.....	11
B. Collecte, de manière incidente, d’informations sur des Canadiens ...	18
1) Introduction.....	18
2) Contexte.....	21

(3) The Service’s practices relating to information about Canadians.....	26	3) Pratiques du Service quant aux informations sur des Canadiens.....	26
(4) Communications and privileges of elected officials.....	49	4) Communications et privilèges des élus.....	49
C. The Relationship Between section 16 and section 12	75	C. Relation entre les articles 12 et 16.....	75
D. Proposed Changes to the section 16 Warrant Templates	93	D. Modifications proposées aux modèles de mandats relatifs à l’article 16.....	93
(1) Incidental changes to warrant templates.....	95	1) Modifications accessoires aux modèles de mandats	95
(2) Clarifying the scope of some powers.....	97	2) Précision de la portée de certains pouvoirs	97
(3) New powers or locations.....	101	3) Nouveaux pouvoirs ou lieux...	101
(4) Conclusion on warrant templates.....	103	4) Conclusion au sujet des modèles de mandats	103
III. Issue Two—Does section 16 authorize use of CSS technology?	104	III. Deuxième question — L’article 16 autorise-t-il le recours aux ESB?	104
IV. Issue Three—Does section 16 authorize interception of [***] data?	126	IV. Troisième question — L’article 16 autorise-t-il l’interception de données [***]?	126
(1) The Technology	130	1) Technologie.....	130
(2) Does section 16 provide sufficient legal authority?.....	149	2) L’article 16 constitue-t-il une autorisation légale suffisante?.....	149
V. Issue Four—Does section 16 authorize interception of communications outside Canada?	182	V. Quatrième question — L’article 16 autorise-t-il l’interception de communications à l’extérieur du Canada?.....	182
VI. Conclusion and Disposition	194	VI. Conclusion et décision	194
I. <u>Background</u>		I. <u>Contexte</u>	

[1] This case began as an application for warrants to gather foreign intelligence pursuant to section 16 of the *Canadian Security Intelligence Service Act*, R.S.C., 1985, c. 23 [CSIS Act or the Act] (see Annex for all provisions cited). It then grew, becoming a vehicle for the consideration of a number of issues that have arisen in the context of section 16 over recent years.

[2] Section 16 grants the Service [Canadian Security Intelligence Service or CSIS] authority to provide assistance to the Minister of National Defence or the Minister of Foreign Affairs by collecting information or intelligence about the capabilities, intentions, or activities of a foreign state or foreign person. The Service’s role under

[1] Une demande de mandats visant la collecte de renseignements étrangers au titre de l’article 16 de la *Loi sur le service canadien du renseignement de sécurité*, L.R.C. (1985), ch. C-23 (Loi sur le SCRS) est à l’origine de la présente espèce (les dispositions citées se trouvent en annexe), qui a ensuite pris de l’ampleur pour devenir un véhicule propice au traitement de questions ayant trait à l’article 16 soulevées au cours des dernières années.

[2] L’article 16 de la Loi sur le SCRS autorise le Service canadien du renseignement de sécurité (SCRS ou Service) à prêter son assistance au ministre de la Défense nationale ou au ministre des Affaires étrangères à la collecte d’informations ou de renseignements sur les moyens, les intentions ou les activités d’un étranger ou

section 16 is distinct from its primary mandate to investigate threats to the security of Canada under section 12 of the CSIS Act.

[3] The original application before me was heard in October 2017. Counsel for the Attorney General of Canada [AGC] had alerted the Court that the application would include submissions on amendments that the Service was seeking to the templates on which section 16 warrants were then based, as well as representations on the treatment of information collected about Canadians, including elected officials, in the course of section 16 investigations. The latter was in response to an earlier Direction from the Court requesting the Service to explain its practices and procedure in a future section 16 warrant application. (I provide further details relating to that Direction below.)

[4] After the October 2017 hearing, I appointed two amici curiae to assist me, Mr. Gordon Cameron and Mr. Owen Rees. (Mr. Rees withdrew as amicus in the fall of 2018 due to a change in his employment). In March 2018, the AGC sought to address other issues that had not been previously considered by the Court in the section 16 context. In addition to the issues relating to the warrant templates and the treatment of information about Canadians, the AGC, jointly with the amici, requested that I address:

- The interplay between section 12 of the CSIS Act and section 16 (this was in response to concerns expressed periodically by the Court).
- Whether section 16 gives lawful authority for the Service to employ cell-site simulator (CSS) technology.
- Whether section 16 gives lawful authority for the Service to conduct [***] surveys.
- Whether section 6 gives lawful authority for the Service to intercept communications of [***foreign persons***] when they are travelling outside of Canada.

d'un État étranger. Ce rôle diffère de celui, fondamental, que l'article 12 de cette même loi confie au Service : enquêter sur les menaces pour la sécurité du Canada.

[3] La demande originale dont j'ai été saisie a été entendue en octobre 2017. L'avocat du procureur général du Canada (procureur général) avait avisé la Cour que la demande serait assortie d'observations portant sur des modifications que le Service voulait apporter aux modèles des mandats relatifs à l'article 16, ainsi que sur le traitement des informations sur des Canadiens, y compris des élus, recueillies dans le cadre d'enquête menée au titre de ce même article. Ce dernier point faisait suite à une directive antérieure par laquelle la Cour avait demandé au Service d'expliquer ses pratiques et procédures dans une future demande de mandats relatifs à l'article 16 (d'autres détails sur cette directive figurent plus loin).

[4] Après l'audience d'octobre 2017, j'ai nommé deux *amici curiae* pour m'aider, MM. Gordon Cameron et Owen Rees (M. Rees a renoncé à ce rôle à l'automne de 2018 en raison d'un changement d'emploi). En mars 2018, le procureur général a cherché à aborder des questions que la Cour n'avait pas encore prises en considération dans le contexte de l'article 16. Outre ce qui concernait les modèles de mandats et le traitement des informations sur des Canadiens, le procureur général, d'un commun accord avec les *amici*, a demandé que je me prononce sur les points suivants :

- l'interaction entre les articles 12 et 16 de la Loi sur le SCRS (en réponse à des préoccupations soulevées périodiquement par la Cour);
- la possibilité que l'article 16 autorise le Service à faire usage d'émulateurs de station de base (ESB);
- la possibilité que l'article 16 autorise le Service à effectuer des sondages [***];
- la possibilité que l'article 16 autorise le Service à intercepter les communications [***des personnes étrangères***] lorsqu'ils se rendent à l'extérieur du Canada.

[5] Shortly thereafter, the AGC filed a number of additional affidavits relating to these issues. A schedule was worked out for the presentation of evidence and oral arguments. A hearing took place in July 2018 and supplementary written submissions were received up until December 2018.

[6] While I have addressed all of the issues presented to me, I should point out that in some areas this judgment is simply a summary of information I received about the Service's section 16 activities that do not require a definitive ruling. For example, in terms of the Service's policies and practices on collecting and retaining information about Canadians, I describe those matters in detail and note the shortcomings that the amici identified. But I did not have a legal basis on which to order the Service to do more. I do, however, point out areas where the Service's policies and practices should be bolstered. Similarly, I describe how the Service carries out parallel operations under sections 12 and 16 and note some concerns about them but, again, found no legal basis for an order.

[7] However, three areas did require rulings—the proposed use of CSS technology, the collection of [***] data, and the interception of [***foreign persons***] communications outside Canada.

[8] I have consolidated the various issues before me under these four headings:

- i. What is the scope of section 16 of the CSIS Act (particularly as it relates to the collection of information about Canadians and to concurrent investigations of threats to the security of Canada under section 12, and the appropriate warrant templates for the execution of intrusive powers in the collection of foreign intelligence)?
- ii. Does section 16 authorize use of CSS technology?

[5] Peu après, le procureur général a déposé un certain nombre d'autres affidavits ayant trait à ces questions. La présentation des éléments de preuve et des observations orales a été mise au rôle. Une audience a été tenue en juillet 2018, et des observations orales supplémentaires ont été déposées jusqu'en décembre 2018.

[6] Dans le présent jugement, j'aborde toutes les questions dont j'ai été saisi. Je souligne toutefois qu'à certains égards, j'y résume simplement des informations dont j'ai pris connaissance à propos des activités menées par le Service au titre de l'article 16, qui ne requièrent pas que je me prononce de manière définitive. À titre d'exemple, je traite en détail de la question des politiques et des pratiques du Service en matière de collecte et de conservation d'informations sur des Canadiens, et je souligne les lacunes relevées par les *amici*. Toutefois, aucun fondement juridique ne m'a permis d'ordonner au Service d'en faire davantage. Je souligne cependant des domaines pour lesquels il y aurait lieu de renforcer les politiques et les pratiques du Service. De même, je décris comment le Service mène parallèlement des opérations au titre des articles 12 et 16 et souligne quelques préoccupations les concernant, mais je n'ai pu constater aucun fondement juridique à une ordonnance.

[7] Par contre, il m'a fallu trancher au sujet de trois questions : l'utilisation proposée d'ESB, la collecte de données [***] ainsi que l'interception de communications [***des personnes étrangères***] à l'extérieur du Canada.

[8] J'ai rassemblé les diverses questions dont je suis saisi sous quatre rubriques :

- i. Quelle est la portée de l'article 16 de la Loi sur le SCRS (relativement, surtout, à la collecte d'informations sur des Canadiens, aux enquêtes menées simultanément sur les menaces pour la sécurité du Canada en vertu de l'article 12 et aux modèles de mandats permettant l'exercice de pouvoirs intrusifs pour la collecte de renseignements étrangers)?
- ii. L'article 16 autorise-t-il le recours aux ESB?

- iii. Does section 16 authorize interception of [***] data?
- iv. Does section 16 authorize interception of [***foreign persons***] communications outside Canada?

- iii. L'article 16 autorise-t-il l'interception de données [***] ?
- iv. L'article 16 autorise-t-il l'interception de communications [***des personnes étrangères***] à l'extérieur du Canada?

[9] In sum, I find that the Service's treatment of information about Canadians, including elected officials is satisfactory, but should be improved. I also conclude that the Service's approach to parallel investigations pursuant to sections 12 and 16 is satisfactory. I have also found that section 16 provides sufficient legal authority to the Service to use CSS technology. However, I find that section 16 does not provide lawful authority to the Service to intercept [***] data; a warrant is required to do so. Finally, I conclude that section 16 authorizes the interception, within Canada, of a [***foreign person's***] communications while outside Canada.

[9] En résumé, je conclus que le traitement des informations sur des Canadiens — dont des élus — par le Service, quoique satisfaisant, requiert des améliorations. J'ajoute que l'approche du Service quant aux enquêtes menées parallèlement au titre des articles 12 et 16 est satisfaisante. En outre, je constate que l'article 16 en soi autorise le Service à utiliser les ESB. Par contre, il ne l'autorise pas à intercepter sans mandat des données [***]. Enfin, je conclus que l'article 16 autorise l'interception, dans les limites du Canada, des communications [***d'une personne étrangère***] qui se trouve à l'extérieur du Canada.

II. Issue One—What is the scope of section 16 of the CSIS Act?

[10] This application requires me to consider the overall scope of section 16 against which some of the more specific questions set out above can be posed. In this section, I begin with some background, then I will discuss the issue of the incidental collection of information about Canadians, including elected officials, in the conduct of section 16 investigations. I will also compare and contrast section 16 with section 12 and discuss the changes that the Service proposes to make to the section 16 warrant templates, largely to bring section 16 warrants into line with section 12 warrants.

A. *Background—The History and Purpose of section 16*

[11] From the beginning—that is, when the CSIS Act was enacted in 1984—the Service was given the express authority, within Canada, to assist the Minister of National Defence and the Minister of Foreign Affairs in gathering information about the “capabilities, intentions or activities” of foreign states or any persons other than Canadian citizens, permanent residents, or corporations

II. Première question — Quelle est la portée de l'article 16 de la Loi sur le SCRS?

[10] La demande en l'espèce exige que je me penche sur la portée générale de l'article 16 en vue de donner réponse à certaines des questions susmentionnées, plus précises. Dans la présente section, je donne d'abord des éléments de contexte, puis je traite de la question de la collecte, de manière incidente, d'informations sur des Canadiens — dont des élus — dans le cadre d'enquêtes menées au titre de l'article 16. En outre, je compare et mets en contraste les articles 12 et 16. J'expose ensuite les modifications que le Service entend apporter aux modèles de mandats relatifs à l'article 16, en vue, surtout, de les aligner sur les mandats liés à l'article 12.

A. *Contexte — Historique et objet de l'article 16*

[11] Dès le départ, c'est-à-dire depuis l'entrée en vigueur de la Loi sur le SCRS en 1984, le Service s'est vu confier le pouvoir exprès de prêter son assistance, dans les limites du Canada, aux ministres de la Défense nationale et des Affaires étrangères à la collecte d'informations sur « les moyens, les intentions ou les activités » d'un État étranger ou d'une personne qui n'entre dans

(paragraphs 16(1)(a),(b)). In this decision, I will refer to this mandate as the Service’s role in gathering “foreign intelligence.”

[12] It was also clear, however, that the need for the Service to be involved in protecting Canada from foreign clandestine activities was merely a secondary role (or even a tertiary one, according to the Special Committee on the Security Intelligence Service, Report of the Special Committee of the Senate on the Canadian Security Intelligence Service. *Delicate Balance: A Security Intelligence Service in a Democratic Society* (Ottawa: Supply and Services Canada), at paragraph 49). See also *X (Re)*, 2018 FC 738, [2019] 1 F.C.R. 567, at paragraph 28; *X (Re)*, 2016 FC 1105, [2017] 2 F.C.R. 396 (*Associated Data*), at paragraph 165.

[13] Nevertheless, section 16 provides broad powers. Arguably, the terms “capabilities, intentions or activities” could refer to virtually anything a foreign country [***or foreign person***] might wish to learn, achieve, obtain, accomplish, or carry out. Further, in pursuit of its section 16 mandate, the Service can request the Court to grant it a range of intrusive powers, including search, seizure, and electronic surveillance, to collect intelligence relating to any of those objects in order to assist one or both of the named ministers.

[14] The range of matters on which a minister might seek assistance is also broad. The mandate of the Minister of Foreign Affairs, for example, includes conducting the external affairs of Canada, as well as international trade, commerce, and development. Global Affairs Canada identifies current priorities as including a comprehensive engagement with countries in the Asia-Pacific Region, as well as diversified international trade and foreign investment. Other notable priorities include combatting drug trafficking, maintaining constructive relations with the United States, and expanding Canadian leadership on the global scene in areas such as human rights, climate change, and peacekeeping. The Minister

aucune des catégories suivantes : les citoyens canadiens, les résidents permanents ou les personnes morales, aux termes des alinéas 16(1)a) et b). Dans la présente décision, il sera question, eu égard à ce rôle du Service, de « collecte de renseignements étrangers ».

[12] Cependant, il était aussi manifeste que la participation du Service à la protection du Canada contre les activités clandestines d’origine étrangère n’était qu’un rôle secondaire (voire tertiaire, selon le Rapport du comité sénatorial spécial sur le Service canadien du renseignement de sécurité. *Équilibre délicat : Un service du renseignement de sécurité dans une société démocratique* (Ottawa : Approvisionnement et Services Canada), au paragraphe 49). Voir aussi *X (Re)*, 2018 FC 738, [2019] 1 R.C.F. 567, au paragraphe 28, et *X (Re)*, 2016 FC 1105, [2017] 2 R.C.F. 396 (*Données connexes*), au paragraphe 165.

[13] Néanmoins, l’article 16 accorde des pouvoirs étendus. Il est possible de soutenir que le segment « les moyens, les intentions ou les activités » renvoie à virtuellement quoi que ce soit qu’un pays [***ou une personne étrangère***] pourrait chercher à apprendre, à atteindre, à obtenir, à accomplir ou à mettre en œuvre. En outre, pour assumer le rôle que lui confère l’article 16, le Service peut demander à la Cour de lui octroyer divers pouvoirs envahissants, par exemple procéder à des fouilles et à des saisies, effectuer de la surveillance électronique et recueillir des renseignements relatifs à n’importe quel de ces objectifs en vue de prêter assistance à l’un ou l’autre des ministres mentionnés.

[14] Les ministres en question peuvent demander de l’assistance sur une vaste gamme de sujets. À titre d’exemple, le ministre des Affaires étrangères est notamment chargé de la conduite des affaires extérieures du Canada, en plus de commerce international et de développement international. Pour l’heure, Affaires mondiales Canada se consacre en priorité à l’établissement d’une collaboration étroite avec des pays de la région de l’Asie-Pacifique et à la diversification du commerce international et des investissements à l’étranger. Le ministère a d’autres priorités dignes de mention : lutter contre le trafic de stupéfiants, entretenir une relation constructive avec les États-Unis et accroître le leadership

also has responsibility for Canada's diplomatic relations, which includes ensuring that foreign diplomats and consular agents in Canada abide by their obligations not to violate Canadian laws or interfere in Canada's internal affairs.

[15] It is perhaps not surprising that the Service scoops up vast quantities of foreign intelligence when it exercises the broad mandate and authority given to it by Parliament under section 16.

[16] At the same time, it is important to recognize that the Service's section 16 mandate contains limits. Its authority to collect foreign intelligence has always been strictly confined to foreign entities, and has precluded the targeting of Canadians. Section 16 allows the Service, within Canada, to gather information or intelligence about a foreign state or group of foreign states, or of a person who is not a Canadian citizen, permanent resident of Canada, or a Canadian corporation. It specifically provides that the Service's assistance cannot be directed at Canadians, whether citizens, permanent residents, or companies (see *Canadian Security Intelligence Service Act (Re)*, 2012 FC 1437, [2014] 2 F.C.R. 514 (*Re CSIS*), at paragraph 98, *per* Justice Anne Mactavish, now a justice of the Federal Court of Appeal). This means that the Service can intercept communications of Canadians under section 16 only incidentally. These incidental interceptions are an inevitable by-product of the collection of foreign intelligence, especially when powers of electronic surveillance are employed.

[17] The Service has an overarching duty to minimize intrusions on the privacy of Canadians who are innocent third parties to a section 16 investigation. Accordingly, the Court requires the Service to provide in advance the names of persons whose communications may be incidentally intercepted (pursuant to *R. v. Chesson*, [1988] 2 S.C.R. 148, (1988), 90 A.R. 347). Where appropriate, the

du Canada sur la scène internationale dans des domaines comme les droits de la personne, les changements climatiques et le maintien de la paix. Le ministre est aussi chargé des relations diplomatiques du Canada. À ce titre, il doit veiller à ce que les diplomates et agents consulaires étrangers au Canada respectent leurs obligations, c'est-à-dire éviter d'enfreindre les lois canadiennes et de s'ingérer dans les affaires internes du pays.

[15] Il n'est donc pas surprenant que le Service recueille de grandes quantités de renseignements étrangers lorsqu'il assume le rôle et exerce les pouvoirs étendus que lui a accordés le législateur au moyen de l'article 16.

[16] Par contre, il est important de reconnaître que le rôle que confère l'article 16 au Service est limité. Son pouvoir de recueillir des renseignements étrangers a toujours été strictement circonscrit aux entités étrangères; il ne peut pas viser des Canadiens. L'article 16 autorise le Service, dans les limites du Canada, à recueillir des informations ou des renseignements sur un État étranger ou un groupe d'États étrangers, ou sur une personne qui n'appartient à aucune des catégories suivantes : citoyens canadiens, résidents permanents du Canada ou personne morale constituée au Canada. Il prévoit précisément que l'assistance prêtée par le Service ne peut pas viser d'entités canadiennes, qu'il s'agisse de citoyens, de résidents permanents ou de sociétés (*Renvoi relatif à la Loi sur le Service canadien du renseignement de sécurité*, 2012 CF 1437, [2014] 2 R.C.F. 514 (*SCRS (Re)*), au paragraphe 98, sous la plume de la juge Anne Mactavish, maintenant à la Cour d'appel fédérale). Partant, le Service ne peut intercepter les communications de Canadiens au titre de l'article 16 que de manière incidente. De telles interceptions sont inévitables dans le cadre de la collecte de renseignements étrangers, surtout lorsqu'il y a exercice de pouvoirs de surveillance électronique.

[17] Le Service est tenu de minimiser le degré d'empiètement sur la vie privée de Canadiens qui sont des tiers innocents dans le cadre d'une enquête menée au titre de l'article 16. Ainsi, la Cour demande au Service de lui fournir à l'avance les noms des personnes dont il pourrait intercepter les communications de manière incidente (conformément à l'arrêt *R. c. Chesson*, [1988]

Court can impose terms or conditions on the execution of a section 16 warrant to curtail excessive intrusions on privacy. However, intrusions on the privacy of targets are significantly greater than intrusions on the privacy of third parties because, unlike targets, their communications cannot be intercepted intentionally (*Re CSIS*, at paragraphs 33–34).

B. Incidental Collection of Information About Canadians

(1) Introduction

[18] The fact that incidental collection of communications by, and information about, Canadians is an inevitable by-product of the collection of foreign intelligence under section 16 has been recognized since the creation of the Service. A proposal that would have required the Service to terminate an interception if a Canadian was a party to the communication was rejected as impractical by the Standing Committee on Justice and Legal Affairs in 1984 (Canada, House of Commons, *Minutes of Proceedings and Evidence*, Issue No. 38 [32nd Parl., 2nd Sess.] (June 7, 1984), at pages 65–68).

[19] At the same time, the collection, retention, and use of incidentally intercepted information raises concerns about Canadians' privacy.

[20] I received a significant amount of evidence about how the Service treats information about Canadians collected incidentally pursuant to section 16. Most of this evidence came in the form of affidavits and testimony from a senior Service employee, the Director General of the Secretariat of Deputy Director Operations (DDO), [***] The following description is taken largely from that person's evidence.

(2) Background

[21] In 2017, my colleague Justice Simon Noël, issued a Direction requesting the Service to provide

2 R.C.S. 148). S'il y a lieu, la Cour peut imposer des conditions à l'exécution d'un mandat relatif à l'article 16 afin de limiter l'empiètement excessif sur la vie privée. Toutefois, le degré d'atteinte à la vie privée est nettement supérieur lorsqu'il s'agit de cibles, car les communications de tiers ne peuvent pas, elles, être interceptées intentionnellement (*SCRS (Re)*, aux paragraphes 33 et 34).

B. Collecte, de manière incidente, d'informations sur des Canadiens

1) Introduction

[18] Le caractère inévitable de l'interception de communications de Canadiens et de l'obtention d'informations sur des Canadiens de manière incidente dans le cadre de la collecte de renseignements étrangers au titre de l'article 16 est un état de fait reconnu depuis la création du Service. Il a été proposé que le Service soit tenu de mettre fin à une interception si un Canadien était impliqué dans la communication visée. Difficilement applicable, cette proposition a été rejetée en 1984 par le Comité permanent de la justice et des affaires juridiques (Canada, Chambre des communes, *Procès-verbaux et témoignages*, fascicule n° 38 [32^e lég., 2^e sess.] (7 juin 1984), aux pages 65 à 68).

[19] Parallèlement, la collecte, la conservation et l'utilisation des informations recueillies de manière incidente soulèvent des préoccupations quant à la vie privée des Canadiens.

[20] J'ai pris connaissance d'une preuve abondante sur la manière dont le Service traite les informations sur des Canadiens recueillies de manière incidente au titre de l'article 16, essentiellement sous forme d'affidavits et de témoignages déposés et livrés par [***] employé haut placé du Service, directeur général du Secrétariat du sous-directeur des Opérations (SDO). Ce qui suit s'inspire en grande partie des éléments de preuve communiqués par cette personne.

2) Contexte

[21] En 2017, mon collègue, le juge Simon Noël, par voie d'une directive, a demandé au Service de fournir

an explanation “as to the CSIS retention practices of Canadians’ communications with [***foreign persons***] and Condition 1 of the General Intercept and Search Warrant.” The Service responded to Justice Noël’s request by way of letter in which it pointed out that section 16 contemplates the incidental collection of information about Canadians as was specifically recognized by Justice Mactavish in her 2011 decision (*Re CSIS*, above). Justice Mactavish found that “properly interpreted, subsection 16(2) prohibits the interception of the communications of [Canadian citizens] ... except insofar as those communications may be incidentally intercepted through the exercise of warrant powers in relation to the communications of [non-Canadians]” (at paragraph 106). Accordingly, said the Service in its reply to Justice Noël, “warrants provide authority to the Service to intercept incidentally the communications and the oral communications of any person solely in the course of exercising the interception powers authorized in the warrants.”

[22] The Service also explained to Justice Noël that the processing of incidentally collected information was conducted promptly and that information that did not fall within the exceptions contained in Condition 1 of the warrants was destroyed [***] Condition 1 states that information about Canadians shall be destroyed unless it (a) relates to activities constituting a threat to national security; (b) could be used to prevent, investigate, or prosecute a crime; or (c) relates to the capabilities, intentions or activities of any foreign state, person, or corporation for which Ministerial assistance has been requested.

[23] According to the Service, information that falls within one of the exceptions in Condition 1 would be retained in accordance with the CSIS Retention Schedule for [***] (although this has since been reduced in practical terms to [***] The information could be used in a report, however, and reports can be retained for 20 to 50 years.

[24] On receiving the Service’s response, Justice Noël issued a further Direction in which he noted that the

des explications sur ses [TRADUCTION] « pratiques de conservation de communications de Canadiens avec [***des personnes étrangères***] ainsi que sur la condition 1 du mandat sur les interceptions générales et les fouilles ». Dans une lettre au juge Noël, le Service a répondu que l’article 16 prévoit la collecte, de manière incidente, d’informations sur des Canadiens, comme l’a reconnu précisément la juge Mactavish en 2011 (*SCRS (Re)*, précitée). Elle a conclu qu’« interprété correctement, le paragraphe 16(2) interdit l’interception des communications [de citoyens canadiens] [...], sauf dans la mesure où ces communications pourraient être interceptées accidentellement dans l’exercice des pouvoirs conférés par mandat à l’égard des communications » de non-Canadiens (*SCRS (Re)*, au paragraphe 106). Partant, selon le Service dans sa réponse au juge Noël, [TRADUCTION] « les mandats confèrent au Service des pouvoirs d’interception; seulement en exerçant ceux-ci, il peut intercepter, de manière incidente, les communications et les communications orales de toute personne ».

[22] Le Service a aussi expliqué au juge Noël qu’il traitait rapidement les informations recueillies de manière incidente et détruisait, [***] toute information échappant aux exceptions prévues à la condition 1 des mandats. En vertu de la condition 1, les informations sur des Canadiens sont détruites à moins qu’elles, selon le cas, a) aient trait à des activités qui constituent une menace pour la sécurité nationale; b) puissent permettre la prévention d’un acte criminel ou servir dans le cadre d’une enquête ou de poursuites relatives à un acte criminel; c) aient trait aux moyens, aux intentions ou aux activités des personnes, personnes morales ou États étrangers au sujet desquels un ministre a demandé l’assistance du Service.

[23] Le Service affirme conserver [***] les informations qui sont des cas d’exception prévus à la condition 1, conformément à son calendrier de conservation (bien que depuis, ce délai ait été réduit en pratique à [***] Toutefois, les informations peuvent faire l’objet de rapports qui, eux, peuvent être conservés de 20 à 50 ans.

[24] Par suite de la réponse du Service, le juge Noël a formulé une autre directive dans laquelle il a souligné

letter “raises questions as to the legitimacy of collection and retention when related to information on Canadians and even more so when such Canadians are democratically elected representatives.” He directed that “this legal issue should be raised as part of a new section 16 warrant application so that the Court can have all the necessary factual and legal information to make a proper determination if required.”

[25] In due course, the Service complied with Justice Noël’s Direction in the application before me. As explained above, the Service also took the opportunity to raise a number of other legal issues arising under section 16.

(3) The Service’s practices relating to information about Canadians

[26] The Service emphasized the scope of the current safeguards in respect of the collection of foreign intelligence pursuant to section 16.

[27] The powers available under section 16 can be invoked only if the Minister of Foreign Affairs or the Minister of National Defence personally requests, in a written Letter of Request, the assistance of the Service. Assistance will be provided only if the Minister of Public Safety and Emergency Preparedness personally responds with a written Letter of Consent.

[28] Attached to the Minister’s Letter of Request is an Annex called “Rationale” setting out the specific intelligence requirements being sought. The Rationale includes “Clear Requirements/Tasking” providing particulars about the matters of greatest interest to the requesting Minister.

[29] Receipt of a Letter of Request does not automatically lead to a Service application for a warrant. Rather, the Service may begin to deploy minimally intrusive measures to gather intelligence—physical surveillance, human source contacts, and so on. If more intrusive tools are needed, the Service may then seek a warrant.

que la lettre [TRADUCTION] « sou[levait] des questions sur la légitimité de la collecte et de la conservation d’informations sur des Canadiens, surtout lorsqu’il s’agit de représentants élus démocratiquement ». Il a demandé que [TRADUCTION] « cette question juridique soit soulevée dans une nouvelle demande de mandats relatifs à l’article 16 afin que la Cour puisse avoir à sa disposition tous les faits et toutes les informations juridiques nécessaires pour se prononcer adéquatement, s’il y a lieu ».

[25] Le Service a fini par se conformer à la directive du juge Noël dans la demande en l’espèce. Comme il en est question plus haut, le Service a profité de l’occasion pour soulever d’autres questions juridiques ayant trait à l’article 16.

3) Pratiques du Service quant aux informations sur des Canadiens

[26] Le Service a mis en relief la portée des mesures de protection en vigueur quant à la collecte de renseignements étrangers au titre de l’article 16.

[27] Le Service ne peut agir au titre de l’article 16 que si la ministre des Affaires étrangères ou le ministre de la Défense nationale lui demande personnellement, par écrit, de lui prêter assistance. L’assistance est subordonnée à une lettre de consentement du ministre de la Sécurité publique et de la Protection civile.

[28] Un document appelé « Justificatif » (« *Rationale* ») est annexé à la lettre de demande. Il établit les exigences spécifiques en matière de renseignement et comporte une rubrique, « Demandes et instructions précises » (« *Clear Requirements/Tasking* »), qui expose en détail les questions qui intéressent particulièrement le ministre demandeur.

[29] Une lettre de demande ne mène pas automatiquement à une demande de mandats par le Service. Celui-ci pourra d’abord utiliser des méthodes de collecte de renseignements minimalement envahissantes, par exemple la filature et le recours à des sources humaines. Il pourra faire une demande de mandats s’il a besoin de recourir à des techniques plus envahissantes.

[30] According to the DDO Directive on Section 16 of the CSIS Act (2014), when the Service receives a request for assistance, it initially examines the request to ensure that it falls within the ambit of section 16, that it does not target Canadians, and that it does not seek information that would normally be obtained under the Service's section 12 mandate (i.e. relating to threats to the security of Canada).

[31] Any information collected pursuant to section 16 is reviewed by a Communications Analyst (CA) who determines whether it has value. If not, the information is destroyed. If so, the CA will draft an internal report which is then reviewed by the CA's supervisor who verifies the relevance of the information, and ensures compliance with the Service's policies. If the report is approved, it is added to the Service's section 16 database.

[32] Internal reports prepared by a CA may form the basis of an external report drafted by a Requirements Officer (RO) whose task is to respond to the Minister's requirements as set out in the Rationale accompanying the Letter of Request. External reports have limited distribution on a need-to-know basis. Recipients must obtain permission from the Service to make further use of them. The level at which approval must be obtained varies according to the sensitivity of the contents of the report.

[33] Information that is collected incidentally about Canadians is protected in a number of ways. To begin with, access to the section 16 database is limited; it is granted only on a file-by-file basis, meaning that persons involved in analyzing foreign intelligence about one country will not have access to information about another. Access is controlled by a senior Service employee, [***]

[34] The Service has also adopted a policy on the minimization of information about Canadians. The DDO Directive on Section 16 of the CSIS Act, cited above, defines minimization as the measures taken to reduce the extent of electronic surveillance while allowing legitimate investigations to be carried out. However, a better

[30] Conformément à la Directive du SDO [sous-directeur des Opérations] par rapport à l'article 16 de la Loi sur le SCRS, datant de 2014, le Service commence par s'assurer que l'aide demandée est visée à l'article 16, ne vise aucun Canadien et ne concerne aucune information dont la collecte relèverait normalement du rôle qui lui est confié par l'article 12 (c'est-à-dire celles qui ont trait aux menaces pour la sécurité du Canada).

[31] Un analyste des communications (AC) examine les informations recueillies au titre de l'article 16. Il détermine si elles sont utiles, sans quoi elles sont détruites. Dans l'affirmative, l'AC rédige un rapport interne qu'il soumet à son superviseur, qui vérifie la pertinence des informations et veille au respect des politiques du Service. Le rapport approuvé est ensuite versé dans la base de données du Service consacrée à l'article 16.

[32] Les rapports internes de l'AC peuvent servir de bases à un rapport externe rédigé par un agent des exigences (AE) chargé de répondre aux besoins exprimés par le ministre dans le Justificatif annexé à la lettre de demande. Les rapports externes ne sont diffusés qu'en fonction du principe du besoin de savoir. Leurs destinataires doivent demander l'autorisation du Service pour en faire un usage quelconque. Le niveau hiérarchique de la personne chargée de donner cette approbation varie en fonction de la sensibilité du contenu.

[33] Les informations sur des Canadiens recueillies de manière incidente bénéficient de diverses mesures de protection. D'abord, l'accès à la base de données consacrée à l'article 16 est limité; il n'est accordé qu'en fonction d'un dossier précis. Autrement dit, quiconque est chargé d'analyser les renseignements étrangers ayant trait à un pays ne pourra pas consulter les informations qui en concernent un autre. [***] qui est un employé haut placé du Service, contrôle l'accès.

[34] Le Service s'est aussi donné une politique sur la divulgation minimale d'informations sur des Canadiens. Selon la Directive du SDO par rapport à l'article 16 de la Loi sur le SCRS, précitée, s'entend par « divulgation minimale » l'adoption de mesures afin de réduire au strict minimum la portée de la surveillance électronique tout

definition of minimization for present purposes is contained in OPS-221, section 1.19:

A term used to identify the practise whereby, unless subject to a specific exemption, any recognizable reference to a Canadian citizen, a permanent resident within the meaning of the *Immigration and Refugee Protection Act (IRPA)* or a corporation incorporated by or under an Act of Parliament or of the legislature of a province or territory, is replaced by a generic term.

[35] In other words, minimization serves to limit disclosure of the identities of Canadians (citizens, permanent residents, and companies) in all section 16 related intelligence by deleting them or replacing them with non-specific labels, such as “a Canadian company” or “a named Canadian person.”

[36] There are four exemptions in OPS-221. Minimization will not occur if the reference to a Canadian:

- i. Is necessary to the understanding or exploitation of the foreign intelligence;
- ii. Concerns activities that could constitute a “[threat] to the security of Canada” as defined in section 2 of the CSIS Act;
- iii. Concerns the prevention, investigation, or prosecution of an alleged indictable offence; or
- iv. Is already in the public domain.

[37] In practice, there is more minimization in external reports than in internal reports. Generally speaking, recipients of external reports do not need to know Canadians’ identities in order to understand or use the intelligence the Service provides in response to a Ministerial request. The main purpose of an external report is to respond to the Rationale contained in the Minister’s Letter of Request; personal information is less likely to be relevant to that purpose. On the other hand, the raw information contained in internal reports will be difficult to understand if the identities of the persons

en assurant l’atteinte des objectifs légitimes d’une enquête. Cependant, le point 1.19 de la politique OPS-221 en donne une définition plus utile en l’espèce :

Expression désignant le principe selon lequel, à moins d’une exemption particulière, toute mention qui permet de reconnaître un citoyen canadien, un résident permanent au sens de la *Loi sur l’immigration et la protection des réfugiés (LIPR)* ou une personne morale constituée en vertu d’une loi fédérale, provinciale ou territoriale est remplacée par un terme général.

[35] Autrement dit, ce principe sert à limiter la divulgation de l’identité de Canadiens (citoyens, résidents permanents et personnes morales) dans tout renseignement lié à l’article 16, soit par suppression ou par remplacement par un terme général, par exemple « une entreprise canadienne » ou « un Canadien connu ».

[36] La politique OPS-221 prévoit quatre exceptions à la divulgation minimale. Une information n’y est pas assujettie si elle :

- i. permet de comprendre ou d’exploiter les renseignements étrangers;
- ii. concerne des activités qui pourraient constituer une « [menace] envers la sécurité du Canada », au sens de l’article 2 de la Loi sur le SCRS;
- iii. peut prévenir un acte criminel présumé ou servir dans le cadre d’une enquête ou de poursuites relatives à un acte criminel présumé;
- iv. peut être obtenue de sources ouvertes.

[37] En pratique, la divulgation minimale s’applique davantage dans les rapports externes que dans les rapports internes. En général, les destinataires de rapports externes n’ont pas besoin de connaître l’identité des Canadiens en cause pour comprendre ou utiliser les renseignements que fournit le Service en réponse à une demande d’un ministre. Un rapport externe vise principalement à répondre aux besoins exprimés par le ministre dans le Justificatif annexé à sa lettre de demande. En cela, les renseignements personnels n’auront vraisemblablement pas une grande utilité. En revanche, les

involved are not disclosed. The Service witness provided examples of internal reports in which the identity of a Canadian was integral to the intelligence that had been gathered; without it, the information would have been virtually useless.

[38] When deciding whether to provide a Canadian's identity in an external report on the grounds that it is necessary to an understanding of the foreign intelligence, ROs do not apply any formal criteria, although the Intelligence Assessment Branch of the Service is developing guidelines. However, ROs do consider the client department receiving the report and the use to which the report will likely be put, and will sometimes limit the distribution of reports containing identifying information, or include a special caveat within the report. The RO's decision not to minimize an identity is reviewed by his or her supervisor.

[39] OPS-221 contains special guidance in respect of Canadian "public officials" and "senior public officials." The former category includes provincial and territorial legislators, mayors, deputy mayors, and municipal council members. The latter consists of a broad range of officials:

Prime Minister, Governor General, Lieutenant Governors, Clerk of the Privy Council, Order-in-Council appointments, Provincial/Territorial Premiers, Provincial/Territorial leaders of opposition parties, Members of Parliament, Senators, Parliamentary/Legislative Secretaries, Deputy Ministers, Associate Deputy Ministers, Assistant Deputy Ministers, heads of public agencies or corporations, members of the Judiciary, and Chiefs of Staff for senior public officials.

[40] The policy requires the approval of the Director of the Service or a designate before any external reports can include information or intelligence relating to public officials or senior public officials (OPS-221, section 3.1).

[41] Where information about a Canadian has been minimized in an external report, the recipient of the

informations brutes que contiennent les rapports internes seront difficiles à comprendre si l'identité des personnes en cause n'est pas révélée. Le témoin du Service a fourni des exemples de rapports internes dans lesquels les informations auraient été pratiquement inutiles si l'identité d'un Canadien n'avait pas été connue.

[38] La décision de l'AE de révéler l'identité d'un Canadien dans un rapport externe parce qu'elle est nécessaire à la compréhension des renseignements étrangers n'obéit à aucun critère officiel. La Direction de l'évaluation du renseignement du Service élabore des lignes directrices à ce sujet. Toutefois, l'AE tient compte du ministère client qui en sera le destinataire ainsi que de l'usage probable qu'il en fera. Partant, il limitera parfois la diffusion d'un rapport contenant des informations qui pourraient permettre de découvrir l'identité d'une personne, ou il y ajoutera une mise en garde spéciale. La décision de l'AE de ne pas appliquer la divulgation minimale est assujettie à l'examen de son superviseur.

[39] La politique OPS-221 donne des directives spéciales ayant trait aux « représentants officiels » et aux « hauts fonctionnaires » canadiens. La première catégorie englobe les membres des corps législatifs provinciaux et territoriaux, les maires, les maires suppléants et les conseillers municipaux. L'autre est assez générale :

Premier ministre, gouverneur général, lieutenant-gouverneur, greffier du Conseil privé, personne nommée par décret, premier ministre provincial et territorial, chef d'un parti d'opposition d'une province et d'un territoire, député fédéral, sénateur, secrétaire parlementaire et d'une assemblée législative, sous-ministre, sous-ministre délégué, sous-ministre adjoint, dirigeant d'un organisme ou d'une société d'État, membre de la magistrature et chef de cabinet d'un haut fonctionnaire.

[40] Conformément à la politique, tout rapport externe devant faire état d'informations ou de renseignements liés à des représentants officiels ou à de hauts fonctionnaires requiert l'approbation préalable du directeur du Service ou d'une personne désignée (point 3.1 de la politique OPS-221).

[41] Le destinataire d'un rapport externe dans lequel les informations sur un Canadien ont fait l'objet d'une

report can request the Service to reveal the identity of the person or company referred to; that is, it can request un-minimization. If the Service agrees to provide that information, it will be contained in a separate report so that the original report containing minimization is not altered; in other words, other recipients of the report will not receive the Canadian's identity.

[42] No particular rationale needs to be given for the un-minimization of information in an external report, and the Service does not apply any specific criteria for granting such a request. However, the standard practice is that the requester must give some reason why a person's identity should be disclosed and provide information about the extent to which that identity will be distributed further. The request is then forwarded to the relevant operational branch for consideration. The branch considers the rationale and the source of the request. It may ask for further information before responding. The branch will also consider whether the minimized identity relates to a source, or could otherwise lead to the identification of a source; if so, the request will be denied. Similarly, if the disclosure would jeopardize an ongoing Service operation, the request will be denied.

[43] The Service's operations relating to section 16 intelligence gathering has been reviewed by the Security Intelligence Review Committee [SIRC] and discussed in various Annual Reports. In the early 1990s, SIRC began examining foreign intelligence retained by the Service (little use had been made of section 16 up to then). It found that the Service was not targeting Canadians or retaining excessive or unnecessary information from section 16 operations ([*Annual Report*] 1993–1994, at page 36).

[44] By the mid-1990s, SIRC was satisfied that the Service was dealing appropriately with information about Canadians, including Canadian political figures, and was reviewing the Service's warrant applications at least annually. The number of section 16 applications was, however, growing.

divulgarion minimale peut demander au Service de révéler l'identité de la personne ou de l'entreprise en cause, c'est-à-dire de renverser la divulgation minimale. Si le Service accède à la demande, les informations seront consignées dans un rapport distinct afin d'éviter que le rapport original soit modifié; autrement dit, les autres destinataires ne seront pas mis au courant de l'identité du Canadien en cause.

[42] Le renversement de la divulgation minimale dans un rapport externe ne nécessite pas de justification particulière, et le Service n'applique aucun critère précis pour accéder à une telle demande. Toutefois, selon la pratique courante, le demandeur doit donner une raison quelconque pour laquelle l'identité devrait être divulguée et préciser jusqu'à quel point cette information sera diffusée par la suite. La demande est ensuite acheminée à la direction opérationnelle compétente pour être étudiée. Celle-ci prend en considération la justification et la source de la demande et peut demander des précisions. Elle tient compte de la possibilité que l'identité visée ait trait à une source ou permette de découvrir l'identité d'une source, ce qui est un motif de rejet de la demande. Le demandeur essuiera également un refus si la divulgation est susceptible de nuire à une opération du Service en cours.

[43] Le Comité de surveillance des activités de renseignement de sécurité (CSARS) a examiné les opérations du Service liées à la collecte de renseignements au titre de l'article 16 et en a traité dans certains rapports annuels. Au début des années 90, le CSARS a commencé à examiner les renseignements étrangers conservés par le Service (jusqu'alors, l'article n'avait été invoqué que rarement). Il a conclu que le Service ne conservait aucune information excédentaire ou inutile découlant des opérations liées à l'article 16 ou de rapports du Centre de la sécurité des télécommunications ([*Rapport annuel*] 1993–1994, à la page 37).

[44] Au milieu des années 90, le CSARS était convaincu que le Service traitait adéquatement les informations sur des Canadiens, y compris des personnalités politiques, et qu'il examinait les demandes de mandats au moins une fois l'an. Cependant, le nombre de demandes faites au titre de l'article 16 croissait.

[45] In the late 1990s, however, SIRC found that there were a number of instances in which the Minister's section 16 requests did not comply with the prohibition on targeting Canadians (1997–1998, at page 53).

[46] In 1999, noting that some section 16 warrants did not contain caveats about the incidental interception of communications by Canadians, SIRC recommended that ministers seeking the Service's assistance should indicate when there is a real likelihood of those interceptions occurring, and that section 16 warrants should explicitly prohibit targeting Canadians (1999–2000, at page 30). SIRC also expressed concern about the duration of the Service's retention of information about Canadians, and suggested that reports to requesting agencies should contain only the information that was absolutely essential for the exploitation of the foreign intelligence.

[47] In the within warrant application, the Service proposes to reinforce its recognition of the limited scope of section 16 in respect of Canadians by adding the following recital indicating that the authorizing judge is satisfied that the section 16 warrant requested is not directed at any Canadians:

I am satisfied that the warrants do not contravene the limitation stipulated at paragraph 16(2) of the *Act*. In particular, I am satisfied that the warrant powers set out herein will not be directed at any person who is a Canadian citizen, a permanent resident within the meaning of the *Immigration and Refugee Protection Act*, or a corporation incorporated by or under an Act of Parliament or of the legislature of a province.

[48] This recital has been included in section 16 warrants over the past year. It is an important addition to these warrants and, in my view, should continue to be employed. This is particularly so given the concerns expressed by SIRC over the years.

(4) Communications and privileges of elected officials

[49] A particular concern relates to the incidental interception of communications between members of

[45] Par contre, à la fin des années 90, le CSARS a constaté des cas où de telles demandes du ministre ne respectaient pas l'interdiction de viser des Canadiens (1997–1998, à la page 53).

[46] En 1999, ayant remarqué que certains mandats relatifs à l'article 16 ne contenaient pas de mise en garde relative à l'interception, de manière incidente, de communications de Canadiens, le CSARS a recommandé que les ministres qui demandent l'assistance du Service précisent, s'il y a lieu, l'existence d'une probabilité réelle que ces interceptions se produisent, et que les mandats interdisent explicitement de prendre des Canadiens pour cible (1999–2000, à la page 30). Le CSARS a aussi soulevé des préoccupations quant à la durée de la période de conservation d'informations sur des Canadiens par le Service et a suggéré que les rapports destinés aux organismes demandeurs contiennent uniquement les informations absolument essentielles à l'exploitation des renseignements étrangers.

[47] Dans la demande de mandats en l'espèce, le Service propose de souligner qu'il reconnaît la portée limitée de l'article 16 en ce qui a trait aux Canadiens par l'ajout, à l'énoncé, d'un paragraphe précisant que le juge saisi de la demande est convaincu que les mandats demandés au titre de l'article 16 ne visent aucun Canadien :

[TRADUCTION] Je suis convaincu que les mandats visés par la présente demande respectent la condition imposée par le paragraphe 16(2) de la Loi *[sur le SCRS]*, plus précisément que les pouvoirs demandés ne seront pas exercés contre des citoyens canadiens, des résidents permanents au sens de la *Loi sur l'immigration et la protection des réfugiés* ou des personnes morales constituées sous le régime d'une loi fédérale ou provinciale.

[48] Cet élément d'énoncé figure dans les mandats décernés au titre de l'article 16 au cours de la dernière année. Il s'agit d'un ajout important qui, à mon avis, devrait demeurer, compte tenu, surtout, des préoccupations soulevées par le CSARS au fil des ans.

4) Communications et privilèges des élus

[49] L'interception, de manière incidente, de communications entre des députés fédéraux ou provinciaux

federal or provincial legislatures and foreign persons or entities. Again, this is an inevitable consequence of foreign intelligence gathering. For example, a [***foreign person***], whose communications are intercepted pursuant to a warrant issued by the Court to the Service, may telephone a member of Parliament to discuss a matter of mutual interest or concern. The member's comments will be intercepted incidentally as a result of the warrant.

[50] The *amici* suggest that these kinds of interceptions do not impinge directly on Parliamentary privilege; however, they maintain that the values that underscore and permeate the concept of Parliamentary privilege are put in play. This requires, they say, special care and treatment of the incidentally intercepted communications.

[51] In my view, parliamentary privilege does not justify the creation of special rules or guidelines to address situations where the communications of elected officials are intercepted pursuant to section 16 warrants. First, properly understood, parliamentary privilege is not engaged by these kinds of interceptions. Second, the Service's current procedures relating to the treatment of incidentally intercepted communications of all Canadians, described above, including public officials and senior public officials, under section 16 warrants are generally adequate and consonant with the Service's section 16 mandate. However, as discussed below, I agree with the *amici* that the Service should develop criteria and guidelines on the unminimization of identifying information about Canadians.

[52] According to the *House of Commons Procedure and Practice*, 2nd ed. [Ottawa: House of Commons], 2009, Parliamentary privilege refers to those rights possessed by members of a legislature that are essential to their role:

Parliamentary privilege is the sum of the peculiar rights enjoyed by each House collectively.... and by Members of each House individually, without which they could not

et des étrangers ou des organisations étrangères souève une préoccupation particulière. Je réitère qu'il s'agit d'une conséquence inévitable de la collecte de renseignements étrangers. À titre d'exemple, il se peut qu'[***une personne étrangère***] dont le Service intercepte les communications en vertu d'un mandat décerné par la Cour, téléphone à un député pour discuter d'une question ou d'une préoccupation d'intérêt mutuel. Le Service interceptera ainsi les propos du député ou du ministre de manière incidente dans l'exécution du mandat.

[50] Selon les *amici*, les interceptions de ce type n'empêchent pas directement sur le privilège parlementaire. Ils soutiennent toutefois qu'elles mettent en cause les valeurs qui sous-tendent et dans lesquelles baigne ce privilège et que, partant, les communications interceptées de manière incidente doivent être traitées avec un soin particulier.

[51] À mon avis, le privilège parlementaire ne justifie pas la création de règles ou de directives spéciales pour le traitement des cas d'interception de communications d'élus au titre de l'article 16. Premièrement, le privilège parlementaire, bien compris, n'est pas mis en cause par ce genre d'interceptions. Deuxièmement, le Service a adopté, pour ce qui est du traitement des communications de Canadiens interceptées de manière incidente au titre de l'article 16, y compris celles de représentants officiels et de hauts fonctionnaires, des procédures (voir plus haut) généralement adéquates qui concordent avec son mandat. Toutefois, comme il en est question plus loin, je conviens avec les *amici* que le Service devrait se donner des critères et des lignes directrices quant au renversement de la divulgation minimale d'informations permettant de reconnaître des Canadiens.

[52] Selon *La procédure et les usages de la Chambre des communes*, 2^e éd., [Ottawa : Chambre des communes], 2009, le « privilège parlementaire » s'entend des droits que détiennent les députés qui sont essentiels à leur rôle :

Le privilège parlementaire est la somme des droits particuliers à chaque chambre, collectivement, [...] et aux membres de chaque chambre, individuellement, faute

discharge their functions, and which exceed those possessed by other bodies or individuals. Thus privilege, though part of the law of the land, is to a certain extent an exemption from the general law.

[53] As an example, to enhance their freedom to debate issues of public policy, legislators are immune from liability for defamation in respect of comments made within the Parliamentary precinct on subjects relating to Parliamentary business. That privilege is limited, and does not extend even to communications between legislators and constituents (*Pankiw v. Canada (Human Rights Commission)*, 2006 FC 1544, [2007] 4 F.C.R. 578).

[54] The question whether the electronic interception of legislators' communications intrudes on Parliamentary privilege has been considered by legislative bodies, but not definitively answered, over the years.

[55] In the late 1970s, the then Speaker of the House of Commons, Mr. James Jerome, ruled that the interception of communications of a Member of Parliament raised a *prima facie* question of privilege, even when it took place outside the Parliamentary precinct, if it amounted to harassment, obstruction, molestation, or intimidation. However, a motion to refer the question to the Standing Committee on Privileges and Elections was defeated in the House, so no formal ruling on the matter was made. (See Special Committee of the Senate on the Canadian Security Intelligence Service, *Proceedings of the Senate on the Canadian Security Intelligence Service on the subject matter of Bill C-157* [32nd Parl., 1st Sess., 1983]; *House of Commons Procedure and Practice*, 2nd ed., 2009, page 9.)

[56] In 1980, a Special Committee of the British Columbia legislature concluded that the interception of a member's communications by the RCMP amounted to a breach of privilege and contempt of the legislature. Fear of intercepts, the Committee found, interfered with members' ability to perform their legislative duties, including in their homes. It stated [at page 2850 of

desquels il leur serait impossible de s'acquitter de leurs fonctions. Ces droits dépassent ceux dont sont investis d'autres organismes ou particuliers. On est donc fondé à affirmer que, bien qu'il s'insère dans l'ensemble des lois, le privilège n'en constitue pas moins, en quelque sorte, une dérogation au droit commun.

[53] À titre d'exemple, pour qu'ils puissent discuter des questions liées aux politiques publiques avec une liberté accrue, les membres des corps législatifs bénéficient d'une immunité contre la diffamation pour les propos qu'ils tiennent dans l'enceinte parlementaire sur des sujets liés aux affaires parlementaires. Il s'agit d'un privilège limité qui ne s'étend même pas aux communications entre ces personnes et leurs électeurs (*Pankiw c. Canada (Commission des droits de la personne)*, 2006 CF 1544, [2007] 4 R.C.F. 578).

[54] Au fil des ans, des corps législatifs ont étudié la possibilité que l'interception électronique des communications de leurs membres empiète sur le privilège parlementaire, mais sans trancher de manière définitive.

[55] À la fin des années 70, le président de la Chambre des communes, M. James Jerome, a statué que l'interception des communications d'un député, même à l'extérieur de l'enceinte parlementaire, soulève une question *prima facie* de privilège et pourrait être considérée comme une forme de harcèlement, d'obstruction de nuisance ou d'intimidation. Toutefois, une motion visant à renvoyer la question au Comité permanent des privilèges et élections a été battue en Chambre. Partant, aucune décision officielle n'a été rendue à ce sujet (Comité sénatorial spécial sur le Service canadien du renseignement de sécurité, *Délibérations du comité sénatorial spécial du Service canadien du renseignement de sécurité sur la teneur du projet de loi C-157* [32^e lég., 1^{re} sess., 1983]; *La procédure et les usages de la Chambre des communes*, 2^e éd., 2009, page 9).

[56] En 1980, un comité spécial du Parlement de la Colombie-Britannique a conclu que l'interception des communications d'un député par la Gendarmerie royale du Canada (GRC) constituait une violation du privilège parlementaire et un outrage au Parlement. Selon le Comité, la crainte de voir leurs communications interceptées empêchait les députés de s'acquitter adéquatement

Legislative Assembly, *Hansard*, 32nd Parl., 2nd Sess., (June 6, 1980):

... parliamentary democracies flourish only when member and constituent can communicate freely, openly and candidly without having the spectre of interception ... interfering with such communications.

[57] Also in 1980, a Special Committee of the Yukon Assembly considered whether the wiretapping of the Minister of Justice's telephone interfered with Parliamentary privilege. Like the B.C. Committee, the Yukon Special Committee concluded that the actions of the RCMP amounted to a breach of privilege and contempt of the House (see Donald E Taylor, "Electronic Surveillance and Members' Privileges" (1989), 12 *Can. Parl. Rev.* 12; David Cheifetz, "Protection of Confidential Communications of Members of Parliament" (1981), 4 *Can. Parl. Rev.* 17).

[58] These events in B.C. and Yukon led the Solicitor General of Canada in 1983 to issue a *Ministerial Directive on Legislators' Privileges and Immunities in relation to Part IV.1 of the Criminal Code within the Precincts of Parliament, Provincial and Territorial Assemblies*. The Directive required the RCMP to seek advance legal advice from the federal or provincial Department of Justice and to inform the agent designated to apply for the warrant that a privilege may be in play. In turn, the agent would have to inform the judge hearing the warrant application of the particular circumstances. Further, the responsible cabinet member—the Solicitor General at the federal level and the Attorney General in the province—was to be informed before the warrant was executed. In addition, if execution of the warrant was to take place within the precincts of Parliament or a legislature, consent of the Speaker would be required.

[59] These examples show special concern about the interception of legislators' communications. None of them, however, involved rulings by the courts on the

de leurs fonctions législatives, y compris à domicile [à la page 2850, Colombie-Britannique, Legislative Assembly, *Hansard*, 32^e lég., 2^e sess., (6 juin 1980)] :

[TRADUCTION] [...] une démocratie parlementaire ne peut s'épanouir que si les députés et leurs électeurs peuvent communiquer librement, ouvertement et franchement sans que la crainte d'une interception [...] ne nuise à leurs communications.

[57] En 1980 également, un comité spécial de l'Assemblée du Yukon s'est penché sur la possibilité que la mise sous écoute de la ligne téléphonique du ministre de la Justice constitue une violation du privilège parlementaire. À l'instar du comité britanno-colombien, le comité spécial du Yukon a conclu que les actions de la GRC constituaient une violation du privilège parlementaire et un outrage à la Chambre (voir Donald E. Taylor, « La surveillance électronique et l'immunité parlementaire » (1989), 12 *Rev. parl. can.* 12; David Cheifetz, « La protection accordée aux communications des députés » (1981), 4 *Rev. parl. can.* 16).

[58] En 1983, ces démarches en Colombie-Britannique et au Yukon ont mené à l'émission, par le Solliciteur général du Canada, de la directive ministérielle sur le privilège et les immunités des membres de corps législatifs, relativement à la partie IV.1 du *Code criminel*, au parlement et dans les enceintes des Assemblées provinciales et territoriales (*Ministerial Directive on Legislators' Privileges and Immunities in relation to Part IV.1 of the Criminal Code within the Precincts of Parliament, Provincial and Territorial Assemblies*). Selon la directive, la GRC devait demander au préalable un avis juridique au ministère de la Justice provincial ou fédéral et informer l'agent chargé de faire la demande de mandats qu'un privilège pouvait être mis en cause. L'agent devait ensuite aviser le juge saisi de la demande des circonstances particulières. En outre, le ministre responsable — le Solliciteur général au fédéral et le procureur général en province — devait être informé au préalable de l'exécution du mandat, et le président de la Chambre devait donner son consentement si le mandat devait être exécuté au parlement ou dans l'enceinte d'une Assemblée.

[59] Ces exemples montrent que l'interception des communications de membres de corps législatifs soulève des préoccupations particulières. Toutefois, aucun d'entre

scope of parliamentary privilege in general, or the impact that intercepting legislators' communications would have on any privilege.

[60] In the United Kingdom, the Investigatory Powers Tribunal considered the issue in 2015: *Caroline Lucas MP and Ors v. Security Service and Ors*, [2015] UKIPTrib 14_79-CH. The Tribunal noted that the general policy, referred to as the “Wilson doctrine”, prohibits interception of parliamentarians' communications. However, according to the Official Guidance given to security services, the Wilson doctrine applies only where the communications of members of parliament are deliberately, not incidentally, targeted. Even so, if special measures are followed, the communications of a Member of Parliament can be targeted and intercepted under warrant. Those measures include special authorization by designated officials, and the involvement of the Secretary of State, the Cabinet Secretary, the Prime Minister, and a special legal advisor charged with retaining and handling the intercepted communications.

[61] Accordingly, notwithstanding the Wilson doctrine, there is no absolute prohibition against the targeted interception of parliamentarians' communications in the United Kingdom, but great care is taken to ensure that interceptions are justified and that their fruits are carefully handled. Note, however, that these U.K. warrants are not subject to judicial authorization.

[62] The Supreme Court of Canada has pronounced on the scope of Parliamentary privilege generally but not on the question of intercepting parliamentarians' communications (*Canada (House of Commons) v. Vaid*, 2005 SCC 30, [2005] 1 S.C.R. 667 [*Vaid*]). At issue in *Vaid* was Parliament's jurisdiction to deal with rights owed to employees of the House of Commons as compared to the jurisdiction of other bodies, such as the Canadian Human Rights Tribunal, with responsibilities for federal public servants generally.

[63] *Vaid* makes clear that defining the scope of Parliamentary privilege falls to the courts, not to the legislatures. The first step is to determine whether “the

eux ne traite des décisions judiciaires ayant trait à la portée du privilège parlementaire en général ni des répercussions qu'aurait l'interception de telles communications sur un quelconque privilège.

[60] Au Royaume-Uni en 2015, l'Investigatory Powers Tribunal (tribunal sur les pouvoirs d'enquête) s'est penché sur la question dans l'affaire *Caroline Lucas MP and Ors v. Security Service and Ors*, [2015] UKIPTrib 14_79-CH. Le Tribunal a souligné que l'approche générale, la « doctrine Wilson », interdisait l'interception des communications de parlementaires. Toutefois, selon la directive officielle donnée aux services de sécurité, la doctrine Wilson s'applique lorsque les communications elles-mêmes sont visées, mais pas lorsqu'elles sont interceptées de manière incidente. Néanmoins, moyennant la prise de mesures spéciales, il est possible de viser et d'intercepter les communications d'un député en vertu d'un mandat. Ces mesures comprennent l'obtention d'une autorisation spéciale par les autorités compétentes, l'implication du secrétaire d'État, du secrétaire du Cabinet, du premier ministre et d'un avocat spécial chargé de conserver et de traiter les communications interceptées.

[61] Partant, au Royaume-Uni, malgré la doctrine Wilson, l'interception ciblée de communications de parlementaires n'est pas frappée d'un interdit absolu, mais un grand soin est apporté à ce que de telles interceptions soient justifiées et que leur produit soit traité avec précaution. Soulignons toutefois que ces mandats britanniques ne sont pas assujettis à une autorisation judiciaire.

[62] Dans l'arrêt *Canada (Chambre des communes) c. Vaid*, 2005 CSC 30, [2005] 1 R.C.S. 667 (*Vaid*), la Cour suprême du Canada s'est prononcée sur la portée du privilège parlementaire en général, mais pas sur la question de l'interception des communications de parlementaires. En cause dans l'arrêt *Vaid* se trouvait la compétence du Parlement quant aux droits reconnus aux employés de la Chambre des communes, par comparaison avec la compétence d'autres instances comme le Tribunal canadien des droits de la personne eu égard aux fonctionnaires fédéraux en général.

[63] Dans l'arrêt *Vaid*, la Cour suprême précise bien qu'il revient aux tribunaux, pas aux corps législatifs, de définir la portée du privilège parlementaire. En premier

existence and scope of the claimed privilege have been authoritatively established” in respect of the Canadian Parliament or the U.K. House of Commons (at paragraph 39). Where there has been no authoritative ruling on the question, the court must “test the claim against the doctrine of necessity, which is the foundation of all parliamentary privilege” (at paragraph 40). While not bound by them, courts will give “considerable deference” to the views of legislators on the scope of autonomy they consider necessary to their function (at paragraph 40).

[64] It is the courts, then, that define the scope of a privilege, while legislators determine the merits or the appropriateness of its exercise.

[65] To determine what is “necessary”, one must consider what is needed “to protect legislators in the discharge of their legislative and deliberative functions, and the legislative assembly’s work in holding the government to account for the conduct of the country’s business” (at paragraph 41). The requirement of necessity imports “important limits” on the scope of the privilege (at paragraph 43). For example, there may be words or actions that are unrelated to parliamentary business and would, therefore, fall outside the parameters of the privilege. Courts will recognize as privileged only those activities that are “so closely and directly connected” with parliamentary functions that “outside interference would undermine the level of autonomy required to enable the assembly and its members to do their work with dignity and efficiency” (at paragraph 46).

[66] In *Vaid*, the Court found that parliamentary privilege did not oust the jurisdiction of the Tribunal, and laid out a number of general principles, the most pertinent of which for present purposes are:

- Parliamentary privilege includes the immunity necessary for members to do their legislative work.

lieu, il faut déterminer « si l’existence et l’étendue du privilège revendiqué ont été établies péremptoirement » en ce qui concerne le Parlement du Canada ou la Chambre des communes britannique (*Vaid*, au paragraphe 39). En l’absence de décision péremptoire, le tribunal doit « déterminer [...] si la revendication satisfait au critère de nécessité qui sert d’assise à tout privilège parlementaire » (*Vaid*, au paragraphe 40). Le tribunal accordera un « grand respect » aux opinions des membres des corps législatifs sur le degré d’autonomie dont ils estiment devoir bénéficier pour s’acquitter de leurs fonctions, bien qu’il ne soit pas lié par ces opinions (*Vaid*, au paragraphe 40).

[64] Partant, la définition de la portée d’un privilège est du ressort des tribunaux, tandis que les membres des corps législatifs en déterminent le bien fondé et l’opportunité de son exercice.

[65] Pour déterminer ce qui est « nécessaire », il est impératif de définir ce qu’il faut pour « protéger les législateurs dans l’exécution de leurs fonctions législatives et délibératives et de la tâche de l’Assemblée législative de demander des comptes au gouvernement relativement à la conduite des affaires du pays » (*Vaid*, au paragraphe 41). L’exigence de nécessité impose « d’importantes limites » à la portée du privilège (*Vaid*, au paragraphe 43). À titre d’exemple, certains mots ou actes peuvent n’avoir aucun trait aux travaux parlementaires et, donc, ne pas être visés par le privilège. Les tribunaux ne considéreront comme visées par le privilège que les activités « si étroitement et directement liées » aux fonctions parlementaires « qu’une intervention externe saperait l’autonomie dont l’assemblée ou son membre ont besoin pour accomplir leur travail dignement et efficacement » (*Vaid*, au paragraphe 46).

[66] Dans l’arrêt *Vaid*, la Cour suprême a conclu que le privilège parlementaire n’écarte pas la compétence du tribunal et a établi des principes généraux, dont voici les plus pertinents en l’espèce :

- Le privilège parlementaire comprend l’immunité dont les députés ont absolument besoin pour effectuer leur travail législatif.

- The test for necessity is what the dignity and efficiency of the House require. The concept of dignity and efficiency is linked to the autonomy that is necessary to enable Parliament and its members to do their jobs.
- The party seeking to rely on the immunity provided by parliamentary privilege has the onus of establishing it.
- Once a category or sphere of activity has been established, it is for Parliament to decide whether the exercise of the privilege is necessary or appropriate.
- Existing categories include: freedom of speech, control by the House over debates and proceedings in Parliament, the power to exclude strangers from proceedings, disciplinary authority over members and non-members who interfere with the discharge of Parliamentary duty, and immunity of members from subpoenas during a parliamentary session.
- The mere affirmation by a legislative body that a certain act is a breach of its privileges will not oust the courts from enquiring and deciding whether the privilege claimed really exists.
- The courts will look more closely at cases in which the privilege claimed will have an impact on persons outside the legislative assembly, than those in which the matters are entirely internal to the legislature.
- Le critère de nécessité consiste à déterminer ce que requièrent la dignité et l'efficacité de la Chambre. Ces deux concepts se rapportent à l'autonomie nécessaire pour que le Parlement et les parlementaires fassent leur travail.
- La partie qui invoque l'immunité que confère le privilège parlementaire a le fardeau d'en établir l'existence.
- Une fois la catégorie ou sphère d'activité établie, c'est au Parlement qu'il revient de décider si l'exercice du privilège est nécessaire ou approprié.
- Les catégories sont notamment la liberté d'expression, le contrôle qu'exercent les Chambres sur les débats ou travaux du Parlement, le pouvoir d'exclure les étrangers des débats, le pouvoir disciplinaire du Parlement à l'endroit des députés et des non-députés qui s'ingèrent dans l'exercice des fonctions du Parlement, y compris l'immunité contre l'arrestation dont jouissent les députés pendant une session parlementaire.
- Le simple fait qu'un corps législatif affirme qu'un acte enfreint ses privilèges n'empêchera pas les tribunaux de se pencher sur la question et de décider si le privilège revendiqué existe réellement.
- Les tribunaux examineront des plus près les affaires dans lesquelles la revendication d'un privilège a des répercussions sur des personnes qui ne sont pas membres de l'Assemblée législative en cause, que celles qui portent sur des questions purement internes.

[67] The Court did not refer to the kind of the privilege discussed above that was recognized in respect of the B.C. and Yukon legislatures; nor did it address the issue of immunity from wiretapping within the categories of privilege currently recognized. But it is clear from its reasoning that it would fall to the courts, not the legislators, to determine whether any such privilege existed. Accordingly, while the views of the B.C. and Yukon

[67] La Cour n'a pas fait allusion au type de privilège susmentionné relativement aux assemblées britannico-colombienne et yukonaise et n'a pas fait figurer la protection contre l'écoute électronique dans les catégories de privilège actuellement reconnues. Cependant, il est clair que, selon son raisonnement, il incomberait aux tribunaux, et pas aux membres d'un corps législatif, de déterminer si un tel privilège existe vraiment. Partant,

legislators merit considerable deference, they are not determinative.

[68] In sum, there is no clear legal authority for the proposition that intercepting the communications of parliamentarians, in itself, violates Parliamentary privilege. Only if the interception interfered with a member's ability to conduct parliamentary business or otherwise constituted harassment or intimidation, would the question of privilege arise.

[69] For section 16 purposes, a parliamentarian, being Canadian, could not be directly targeted. However, as mentioned, his or her communications could be intercepted incidentally pursuant to a valid section 16 foreign intelligence warrant. Not being a target, it is difficult to see how an interception could amount to an attempt to interfere with the member's ability to conduct parliamentary business. Similarly, if the member is not the target, it is unlikely that the execution of the warrant would take place within the Parliamentary precinct. There would be no need to obtain the permission of the Speaker of the House to conduct an interception.

[70] In any case, however, as explained above, the *amici* do not assert that parliamentarians enjoy actual immunity from incidental interceptions of their communications in the foreign intelligence gathering context. Therefore, I need not rule definitively on that question. I do, however, have to consider whether applications for, and the fruits of, those interceptions require special treatment.

[71] The *amici* suggest that the current policies that apply to the incidental interception of parliamentarians' communications provide inadequate protection of Canadians' privacy. They propose that the Court impose conditions on the Service relating to the retention, disclosure, and minimization of information about elected officials pursuant to the authority to include terms and conditions on the execution of warrants issued by the Court (CSIS Act, paragraph 21(4)(f)). They also suggest

bien qu'elles méritent un grand respect, les opinions des membres des corps législatifs de Colombie-Britannique et du Yukon ne sont pas déterminantes.

[68] En somme, il n'existe aucun fondement juridique clair à l'hypothèse selon laquelle l'interception des communications de parlementaires constitue en soi une violation du privilège parlementaire. La question du privilège ne serait soulevée que si l'interception nuisait au député dans l'exercice de ses fonctions parlementaires ou constituait autrement du harcèlement ou de l'intimidation.

[69] Un parlementaire canadien ne pourrait pas être directement visé par des activités menées au titre de l'article 16. Toutefois, comme il a été mentionné, ses communications pourraient être interceptées de manière incidente en vertu d'un mandat relatif à l'article 16 valide en matière de renseignement étranger. Il est difficile de concevoir comment une telle interception pourrait être assimilée à une tentative de nuire au député dans l'exercice de ses fonctions parlementaires, puisqu'il n'est pas une cible. En outre, cet état de fait rend peu probable l'exécution du mandat dans l'enceinte parlementaire. Il n'y aurait aucun besoin de demander l'autorisation du président de la Chambre pour effectuer une interception.

[70] De toute façon, comme il a été expliqué, les *amici* ne soutiennent pas que les parlementaires jouissent effectivement de l'immunité contre l'interception, de manière incidente, de leurs communications dans le contexte de la collecte de renseignements étrangers. Partant, je n'ai pas à me prononcer de façon définitive sur la question. Par contre, je dois déterminer si les demandes d'interception et le produit de ces interceptions doivent recevoir un traitement spécial.

[71] Les *amici* sont d'avis que les politiques en vigueur qui s'appliquent à l'interception, de manière incidente, des communications de parlementaires ne protègent pas bien la vie privée des Canadiens. Ils proposent que la Cour impose des conditions au Service en matière de conservation, de communication et de divulgation minimale d'informations concernant des élus, en vertu du pouvoir que lui confère l'alinéa 21(4)f) de la Loi sur le SCRS d'ajouter des conditions à l'exécution

that the Court play a supervisory role. In particular, they submit that the Service should be required to return to the Court for permission to retain incidentally collected communications of Canadians, to distribute information collected, or to unminimize the identities of Canadians. They note that, in the case of incidental collection of communications of elected officials, these requirements would permit the Court to rule on any issues of parliamentary privilege that might arise. While they do not see the need for special rules for parliamentarians, they note that clearer rules about Canadians generally would also foster communications between elected officials and their constituents.

[72] I largely agree with the *amici*. Greater protection should be granted to information about Canadians incidentally collected in the gathering of foreign intelligence. As mentioned, there are no formal criteria guiding Service employees or others on unminimizing identities of Canadians. Without guidelines, decisions about the retention, disclosure, and distribution of this information is left to individual discretion. More is required, especially since this is information that is acquired merely as a by-product of the Service's mandate to collect foreign intelligence. I would not go so far, however, as to impose a blanket obligation on the Service to return to the Court for permission to retain incidentally collected information about Canadians.

[73] The information about Canadians that the Service obtains in this fashion merits special care and respect. That is even more true for information about public officials and senior public officials, as the Service's policies already recognize. As explained, it is not parliamentary privilege itself that animates the need for extra care; indeed, few officials could mount any real claim to privilege. The concern about gathering information about public officials is that the Service may be intercepting highly sensitive communications emanating from persons charged with the governance of Canada. That

d'un mandat qu'elle décerne. Ils suggèrent également à la Cour de jouer un rôle de supervision. À leur avis, en particulier, le Service devrait être tenu de présenter une nouvelle demande à la Cour pour être autorisé à conserver les communications de Canadiens recueillies de manière incidente, pour diffuser les informations ainsi recueillies ou pour renverser la divulgation minimale d'informations permettant de reconnaître des Canadiens. Ils soulignent que, s'agissant de communications d'élus interceptées de manière incidente, ces exigences permettraient à la Cour de trancher toute question touchant le privilège parlementaire. Bien qu'ils ne voient pas la nécessité de règles spéciales eu égard aux parlementaires, ils soulignent que des règles plus précises au sujet des Canadiens en général favoriseraient aussi les communications entre les élus et leurs électeurs.

[72] Je souscris en grande partie à l'opinion des *amici*. Il y a lieu d'accroître la protection accordée aux informations sur des Canadiens recueillies de manière incidente dans le cadre de la collecte de renseignements étrangers. Comme je l'ai mentionné, aucun critère officiel ne guide les employés du Service — entre autres — en ce qui a trait au renversement de la divulgation minimale de l'identité de Canadiens. Sans lignes directrices, les décisions sur la conservation, la communication et la diffusion de ces informations relèvent de la discrétion de chacun. Ce n'est pas suffisant, surtout que ces informations ne sont que des sous-produits de la collecte de renseignements étrangers par le Service. Toutefois, je n'irais pas jusqu'à imposer au Service l'obligation générale de redemander à la Cour l'autorisation de conserver les informations sur des Canadiens recueillies de manière incidente.

[73] Les informations sur des Canadiens que le Service obtient ainsi méritent d'être traitées avec un soin particulier, à plus forte raison celles qui touchent des représentants officiels et de hauts fonctionnaires, comme le reconnaissent déjà les politiques du Service. Comme cela a été expliqué, la nécessité d'un soin accru n'est pas liée au privilège parlementaire en soi; en effet, peu de ces représentants pourraient réellement l'invoquer. La préoccupation relative à la collecte d'informations sur ces représentants tient à la possibilité que le Service intercepte des communications très sensibles de

information, particularly information about the identity of the Canadian persons involved, must be carefully handled.

[74] In my view, the Service must develop guidelines for distributing and unminimizing the identities of Canadians whose communications have been incidentally intercepted. It should advise the Court of the content of those guidelines and permit the Court an opportunity to comment on them. In individual warrant applications, the Service should continue to inform the Court when there may be incidental interceptions of Canadians' communications. It should also specifically disclose when there is a possibility that the communications of an elected official or other public servant may be intercepted. This disclosure requirement will permit the Court, where appropriate, to attach terms and conditions on the execution of the warrants it issues. Those terms and conditions could include imposing a requirement on the Service to return to the Court for directions on the handling of information collected, as proposed by the *amici*.

C. The Relationship Between section 16 and section 12

[75] An ongoing concern of members of the Court is the potential overlap between, or the blending of, the Service's mandates under section 16 and section 12. Accordingly, I asked the Service to address this issue based on the observation that some recent requests for warrants under section 16 for foreign intelligence purposes resemble applications under section 12 for warrants to investigate threats to national security. The resemblance arises from two features of these section 16 applications. First, they have related, in essence, to matters that could easily be described as threats to the security of Canada. Second, they sometimes involve targets who are already the subject of warrants under section 12.

[76] The concern that arises from this situation is that section 16 could come to be used as an alternative or a supplement to section 12, contrary to the intention of

personnes chargées de la gouvernance du Canada. Ces informations, surtout celles qui concernent l'identité des Canadiens qui ont pris part à la communication, doivent être traitées avec soin.

[74] J'estime que le Service doit se donner des lignes directrices sur la diffusion d'informations pouvant permettre de reconnaître des Canadiens dont les communications ont été interceptées de manière incidente et sur le renversement de la divulgation minimale les concernant. Il devrait informer la Cour de la teneur de ces lignes directrices et lui donner l'occasion de les commenter. Dans chaque demande de mandats, le Service devrait continuer d'informer la Cour des cas possibles d'interception, de manière incidente, de communications de Canadiens, particulièrement s'il peut s'agir d'élus ou de fonctionnaires. Au besoin, la Cour pourra ainsi fixer des conditions à l'exécution des mandats qu'elle décerne. À titre d'exemple, comme l'ont proposé les *amici*, elle pourrait imposer au Service de lui redemander des directives sur le traitement des informations recueillies.

C. Relation entre les articles 12 et 16

[75] Le possible chevauchement des rôles confiés au Service par les articles 12 et 16, voire la confusion entre les deux, constitue une préoccupation permanente des juges de la Cour. Partant, j'ai demandé au Service d'étudier la question, compte tenu du fait que certaines demandes de mandats récemment faites au titre de l'article 16 en matière de renseignement étranger ressemblaient à des demandes de mandats relatives à des enquêtes sur des menaces pour la sécurité nationale, qui relèvent de l'article 12. La ressemblance découle de deux caractéristiques de ces demandes de mandats faites au titre de l'article 16. D'abord, elles portaient essentiellement sur des questions qui passeraient facilement pour des menaces pour la sécurité du Canada. Ensuite, elles mentionnaient des cibles qui faisaient déjà l'objet de mandats décernés au titre de l'article 12.

[76] Cette situation est préoccupante en ce sens que l'article 16 pourrait finir par servir de solution de rechange ou de complément à l'article 12, contrairement

Parliament when enacting the CSIS Act. When requesting a warrant, the Service may sometimes perceive an advantage in proceeding under section 16 rather than section 12. Section 16 arguably has a broader scope relating as it does to the collection of information about “the capabilities, intentions or activities” of any foreign state or non-Canadian person. By contrast, section 12 applies only to the collection, analysis, and retention of information relating to “threats to the security of Canada”, a term that is statutorily defined.

[77] A potential scenario would be this: If the Service believed that a foreign person in Canada was involved in some activity that posed a danger that did not necessarily fall within the definition of a “[threat] to the security of Canada,” it could seek a warrant under section 16 to determine the person’s intentions, capabilities, or activities. Of course, there are constraints that apply to section 16. The Service could seek a foreign intelligence warrant only if its assistance was requested by the Minister of National Defence or the Minister of Foreign Affairs, and with the consent of the Minister of Public Safety and Emergency Preparedness. Further, the Service could collect information only within Canada. The Service could not directly target a Canadian person. However, if a Canadian was known to be in contact with [***] or other foreign persons, the Service could target the latter and “incidentally” intercept the communications of the former. In effect, a Canadian could become the indirect target of a foreign intelligence warrant, even though section 16 specifically prohibits the targeting of Canadians.

[78] I hasten to point out that there is no suggestion that the Service has ever used section 16 in this manner. The concern arises from the potential to use section 16 in this way and, as mentioned, the facial similarity between some recent section 16 applications and section 12 requests.

à l’intention du législateur à l’adoption de la Loi sur le SCRS. Lorsqu’il demande un mandat, il peut arriver que le Service considère qu’invoquer l’article 16 plutôt que l’article 12 présente un avantage. On peut soutenir que l’article 16 offre à la collecte d’informations une portée plus étendue, car celles-ci concernent « les moyens, les intentions ou les activités » de tout État étranger ou de tout non-Canadien. En revanche, l’article 12 ne touche qu’à la collecte, à l’analyse et à la conservation d’informations sur des « menaces envers la sécurité du Canada », terme défini dans la Loi sur le SCRS.

[77] Voici un cas de figure possible, à titre d’exemple. Le Service pourrait faire une demande de mandats au titre de l’article 16 pour prendre connaissance des intentions, des moyens ou des activités d’un étranger qu’il estime être impliqué, au Canada, dans une activité qui constitue un danger, mais à laquelle la définition de « [menace] envers la sécurité du Canada » ne s’applique pas nécessairement. Bien sûr, l’article 16 ne vient pas sans contraintes. Le Service ne peut demander un mandat relatif au renseignement étranger que si le ministre de la Défense nationale ou des Affaires étrangères lui a demandé de lui prêter son assistance, et uniquement avec le consentement du ministre de la Sécurité publique et de la Protection civile. En outre, le Service ne recueillerait des informations que dans les limites du Canada. Il ne pourrait pas viser directement un Canadien, mais s’il savait qu’un Canadien était en contact avec [***] ou d’autres étrangers, le Service pourrait viser cet État ou cet étranger et intercepter « de manière incidente » les communications du Canadien en question. Dans les faits, un Canadien pourrait devenir la cible indirecte d’un mandat relatif au renseignement étranger, même si celui-ci interdit expressément que des Canadiens soient pris pour cible.

[78] Je m’empresse de préciser que rien ne porte à croire que le Service a déjà fait un tel usage de l’article 16. La préoccupation émane de la possibilité que cela puisse être et, comme je l’ai mentionné, de la ressemblance apparente entre de récentes demandes de mandats relatives à l’article 16 et les demandes de mandats faites au titre de l’article 12.

[79] The Service addressed this issue by presenting the evidence of two senior and experienced Service members. This evidence satisfies me that the Service has taken steps to ensure that there is no operational interaction between the Service's foreign intelligence activities under section 16 and its section 12 mandate relating to security intelligence. The following is a summary of that evidence.

[80] The Service's operations, whether under section 12 or section 16, or otherwise, are subject to internal policy directions. For matters relating to national security, if the Service has grounds to suspect that a person or group poses a threat, it may request internal authority to begin an investigation. Those charged with reviewing these requests help ensure that the proposed investigation complies with the Service's policies and the governing law, and amounts to a proportional response to the perceived threat.

[81] Information collected under section 12 is reviewed by an analyst who determines its intelligence value. Information is retained only as permitted by the Service's retention schedule. Information with no intelligence value is destroyed after [***] Valuable information may be retained for 20 or 25 years after the last action on the file. Information that was collected pursuant to a warrant is subject to the conditions set out in it. For example, specific time periods for destruction of information are provided for solicitor-client communications and the communications of third parties.

[82] Policies also govern the preparation of operational reports. If the analyst concludes that the information collected is valuable, and that the applicable policies and conditions have been respected, he or she will prepare an operational report. These reports are reviewed by supervisors who verify the relevance of the information collected, ensure that the Service's policies have been respected and, if the information was gathered under a warrant, confirm compliance with the applicable terms and conditions. If the supervisor approves the report, it

[79] Le Service a abordé la question au moyen des témoignages de deux employés haut placés et expérimentés au Service, qui m'ont convaincu que le Service a pris des mesures pour qu'il n'y ait aucune interaction de nature opérationnelle entre les activités de renseignement étranger qu'il mène en lien avec l'article 16 et le mandat que lui donne l'article 12 en matière de renseignement de sécurité. Voici un résumé de ces témoignages.

[80] Les opérations du Service, qu'elles relèvent de l'article 12 ou de l'article 16 ou qu'elles soient d'une autre nature, sont assujetties à des politiques internes. S'il existe des motifs raisonnables de croire qu'une personne ou un groupe représente une menace pour la sécurité nationale, une demande d'autorisation d'enquête peut être présentée aux autorités compétentes au sein du Service. Celles-ci veillent à ce que l'enquête soit conforme aux politiques du Service et aux lois applicables et constitue une réaction adaptée à la menace perçue.

[81] Un analyste examine les informations recueillies en vertu de l'article 12 pour en déterminer l'utilité sur le plan du renseignement. Le Service les conserve uniquement pendant la période prévue dans son calendrier de conservation. Celles qui n'ont pas d'utilité sur le plan du renseignement sont détruites [***] suivant la collecte. Les informations utiles peuvent être conservées pour 20 ou 25 ans après la date de la dernière intervention au dossier. Les informations recueillies en vertu d'un mandat sont assujetties aux conditions qui y figurent. À titre d'exemple, des délais précis s'appliquent à la destruction des communications entre un avocat et son client et des communications de tiers.

[82] Des politiques régissent également la production des rapports opérationnels. L'analyste prépare un tel rapport après avoir conclu que les informations recueillies sont utiles et que les conditions et politiques applicables ont été respectées. Le rapport passe ensuite entre les mains d'un superviseur, qui vérifie la pertinence des informations, s'assure du respect des politiques du Service et, si les informations ont été recueillies en vertu d'un mandat, confirme que les dispositions et les conditions en ont été respectées. Le

will be stored in the Service's section 12 database. These reports may then form the basis of other intelligence reports submitted to persons within the Government of Canada, with the caveat that they not be used or distributed further without the Service's permission.

[83] Information collected under section 16 is treated similarly, but separately. Again, an investigation must first be authorized. Here, though, that authority comes from the Minister of Public Safety's consent to a written request for assistance from the Minister of Foreign Affairs or the Minister of National Defence. Once the Service receives the request and the consent, it will begin gathering relevant information and, if there are reasonable grounds to believe that the powers available under warrant are necessary, it will seek the Court's authority under section 21 of the CSIS Act.

[84] The Service itself recognizes the possibility of a co-mingling of section 12 and section 16 mandates. The Service's operations policy acknowledges that parallel investigations may be necessary in some circumstances; however, it specifically provides that "operations conducted to support an investigation under one section of the CSIS Act will not be used as a pretext for conducting operations pursuant to another section of the *Act*" (emphasis in the original).

[85] Over the years, the Security Intelligence Review Committee has repeated similar concerns.

[86] In 2006–2007, SIRC reported that the Inspector General had noted considerable overlap between section 12 and section 16 operations. For example, agents tasked with obtaining information abroad under section 12 provided intelligence relevant to section 16. Indeed the Inspector General wondered whether the geographical constriction of section 16 ("within Canada") was a meaningful limitation on the Service's powers (page 37).

rapport approuvé est ensuite versé dans les bases de données du Service ayant trait à l'article 12 et peut servir de matière première à des rapports de renseignement destinés à des intervenants au gouvernement fédéral, qui se voient signifier de ne pas les utiliser ni les diffuser plus avant sans l'autorisation du Service.

[83] Les informations recueillies au titre de l'article 16 subissent, séparément, un traitement similaire. Encore une fois, l'enquête doit d'abord être autorisée. En l'occurrence, toutefois, l'autorisation découle du consentement que donne le ministre de la Sécurité publique à la demande d'assistance présentée par écrit par le ministre des Affaires étrangères ou de la Défense nationale. Une fois la demande et le consentement reçus, le Service commence la collecte d'informations pertinentes. S'il a des motifs raisonnables de croire qu'il a besoin des pouvoirs prévus dans des mandats, le Service en fait la demande à la Cour en vertu de l'article 21 de la Loi sur le SCRS.

[84] Le Service reconnaît la possibilité qu'il y ait confusion entre les rôles que lui confèrent les articles 12 et 16. Ses politiques opérationnelles prévoient que des enquêtes parallèles peuvent être nécessaires en certaines circonstances. Cependant, elles prévoient spécifiquement que [TRADUCTION] « les opérations menées à l'appui d'une enquête visée à un article de la Loi sur le SCRS ne doivent pas servir de prétexte à la conduite d'opérations en application d'un autre article de cette même *loi* » (souligné dans l'original).

[85] Au fil des ans, le CSARS a réitéré de semblables préoccupations.

[86] En 2006–2007, le CSARS a signalé que l'inspecteur général avait remarqué des chevauchements considérables entre des opérations menées au titre de l'article 12 et de l'article 16. À titre d'exemple, des agents chargés d'obtenir des informations à l'étranger en vertu de l'article 12 fournissaient des renseignements visés à l'article 16. L'inspecteur général s'est même questionné sur la portée de la restriction géographique prévue à l'article 16 (« dans les limites du Canada ») quant aux pouvoirs du Service (à la page 37).

[87] Further, in 2009–2010, SIRC noted that the Service had referred to simultaneous section 16 and section 12 investigations as “blended collections”, where the Service was engaged in section 12 and section 16 operations against the same targets. It observed that if this situation were to continue, the Service could become a body with equivalent foreign intelligence and security intelligence mandates, which was not the original intention of Parliament. It recommended that the Government of Canada provide direction or guidance to the Service on its expanded role in collecting foreign intelligence (2009–2010, at page 15).

[88] In 2013, SIRC again detected a potential tension between the Service’s two mandates under sections 12 and 16. The Service itself felt its section 16 non-threat-related mandate had the potential to distract it from its primary role of gathering threat-related intelligence under section 12 (2012–2013, at page 16).

[89] In 2015, SIRC commended the Service for adapting its section 16 procedures to coordinate and streamline its priorities and activities. The Service had also made changes to distinguish between its section 12 and section 16 operations (2014–2015, at page 22).

[90] The *amici* emphasize that the Service must not make any “colourable use” of a section 16 foreign intelligence warrant to collect section 12 security intelligence. This means that the Service should seek a separate section 12 warrant if its section 16 investigation discloses a threat to national security. In addition, where parallel investigations are ongoing, the Service must satisfy the discrete requirements for section 12 and section 16 warrants separately and independently, and inform the judge receiving each warrant application of the existence of the other.

[87] En outre, en 2009–2010, le CSARS a souligné que le Service avait qualifié de [TRADUCTION] « collectes mixtes » des enquêtes menées simultanément au titre des articles 12 et 16, lorsque des opérations effectuées au titre des deux articles avaient les mêmes cibles. Le CSARS a fait observer que, si la situation perdurait, le Service pourrait devenir un organisme ayant des rôles équivalents en matière de renseignement étranger et de renseignement de sécurité, ce qui n’était pas l’intention originale du législateur. Il a recommandé que le gouvernement du Canada offre une orientation ou des conseils au Service au sujet de son rôle accru dans la collecte de renseignements étrangers (2009–2010, à la page 15).

[88] En 2013, le CSARS a de nouveau détecté un conflit possible entre les rôles confiés au Service par les articles 12 et 16. Le Service lui-même estimait que ses fonctions visées à l’article 16, qui ne concernent pas la menace, étaient susceptibles de le détourner de son rôle premier, à savoir recueillir des informations liées à la menace en vertu de l’article 12 (2012–2013, à la page 16).

[89] En 2015, le CSARS a félicité le Service pour avoir adapté ses procédures relatives à l’article 16 afin de coordonner et de simplifier ses priorités et ses activités. Le Service avait aussi apporté des changements en vue d’établir une distinction entre les opérations qu’il menait au titre des articles 12 et 16 (2014–2015, à la page 22).

[90] Les *amici* insistent pour dire que le Service ne doit faire aucun [TRADUCTION] « usage valable en apparence » d’un mandat décerné au titre de l’article 16 pour recueillir des renseignements de sécurité en vertu de l’article 12. Cela signifie que le Service devrait demander un mandat distinct au titre de l’article 12 si son enquête liée à l’article 16 révélait une menace pour la sécurité nationale. En outre, en cas d’enquêtes parallèles, le Service doit satisfaire aux exigences propres aux mandats relatifs à l’un et à l’autre article de manière distincte et indépendante, et informer le juge saisi de chaque demande de l’existence de l’autre.

[91] The *amici* accept, based on the evidence filed on this application, that the Service is currently abiding by the procedures they propose. They note, however, that the heightened protection in respect of incidentally collected information about Canadians that they recommend (as discussed above) would help ensure that the Service does not use foreign intelligence warrants to collect security intelligence about Canadians.

[92] In my view, the Service is acutely aware of the Court's (and SIRC's) concerns in this area. It has addressed those concerns in a serious way in both its operations and policies. I see no need to propose any further action on the Service's part. I have no doubt, however, that members of the Court will continue to expect the Service to address any concerns the Court may have about future "blended collections." In addition, I agree with the *amici* that stronger protection in respect of incidentally collected information about Canadians would help dispel some of those concerns.

D. Proposed Changes to the section 16 Warrant Templates

[93] The AGC proposes a number of changes to the templates that provide a presumptive format and content for the various kinds of foreign intelligence warrants the Court issues pursuant to section 16. These changes fall within three categories:

- i. Incidental changes bringing the section 16 warrant templates into line with section 12 warrants.
- ii. Amendments clarifying the scope of particular powers.
- iii. New powers.

[94] In this section, I will deal only with proposed changes that do not amount to any significant expansion of the powers exercised under section 16 warrants. I will deal elsewhere with the comparatively substantial

[91] Compte tenu de la preuve en l'espèce, les *amici* admettent que le Service suit actuellement les procédures proposées. Toutefois, ils soulignent que les mesures de protection renforcées ayant trait aux informations sur des Canadiens recueillies de manière incidente qu'ils recommandent (voir plus haut) aideraient à assurer que le Service n'utilise pas de mandats sur le renseignement étranger pour recueillir des renseignements de sécurité sur des Canadiens.

[92] À mon avis, le Service est parfaitement au courant des préoccupations de la Cour (et du CSARS) à cet égard. Il en a tenu compte avec sérieux tant dans ses opérations que dans ses politiques. Je ne crois pas qu'il soit nécessaire de proposer l'adoption d'autres mesures par le Service. Par contre, je n'ai aucun doute que les juges de la Cour continueront de s'attendre à ce que le Service réponde à toute préoccupation qu'elle pourra avoir au sujet de toute « collecte mixte ». En outre, je conviens avec les *amici* que des mesures de protection rigoureuses quant aux informations sur des Canadiens recueillies de manière incidente aideraient à dissiper certaines de ces préoccupations.

D. Modifications proposées aux modèles de mandats relatifs à l'article 16

[93] Le procureur général propose une série de modifications aux modèles (format et contenu) des différents mandats sur le renseignement étranger que décerne la Cour au titre de l'article 16. Il y en a trois catégories :

- i. les modifications accessoires permettant d'aligner les modèles de mandats relatifs à l'article 16 sur ceux liés à l'article 12;
- ii. la précision de la portée de certains pouvoirs;
- iii. les nouveaux pouvoirs.

[94] Ci-dessous, je n'aborde que les modifications proposées qui n'élargissent pas de manière importante les pouvoirs exercés en vertu des mandats relatifs à l'article 16. Je traiterais plus loin des changements plus

changes the Service seeks, such as those relating to the use of CSS and [***] surveys.

(1) Incidental changes to warrant templates

[95] The Service proposes a number of amendments that would bring section 16 warrant templates in line with section 12 templates. These include:

- Inclusion of a new condition clarifying the meaning of the word “destroyed” when creating an obligation on the Service to destroy information. “Destroyed” would be defined as meaning that the information “shall not be retrieved by the Service or by any other agency or person on its behalf.”
- Amendment of the definition of “residence” to include any place in which a Regional Director General has reasonable grounds to believe a person resides.
- Inclusion of a definition of “test data” and a corresponding condition allowing the Service to retain intercepted communications solely for purposes of developing or maintaining its interception and collection capabilities.
- Replacing the definition of [***] with [***] to provide a more accurate description of the means used to locate a person or vehicle [***]
- Expanding the description of places where warrants can be executed to include [***]
- Adding a power to intercept [***]
- Adding a power to obtain images of persons named in the warrant or attending places specified in the warrant.
- Amending the retention condition of the warrants by including an assessment period of [***]

importants que souhaite apporter le Service, par exemple en ce qui a trait à l’utilisation d’ESB et au sondage [***]

1) Modifications accessoires aux modèles de mandats

[95] Le Service propose des modifications destinées à aligner les modèles de mandats liés à l’article 16 sur ceux liés à l’article 12 :

- Ajouter une condition précisant la définition du terme « détruire » lorsqu’il y a obligation, pour le Service, de détruire des informations. Ainsi, les informations détruites ne pourront être récupérées ni par le Service ni par un organisme ou une personne agissant en son nom.
- Modifier la définition de « domicile » pour qu’elle inclue tout lieu où un directeur général régional a des motifs raisonnables de croire qu’une personne réside.
- Ajouter une définition de « données d’essai » et une condition correspondante autorisant le Service à conserver les communications interceptées à la seule fin de perfectionner ou d’entretenir ses solutions d’interception et de collecte.
- Remplacer le terme [***] et sa définition par [***] qui décrit plus précisément les moyens utilisés pour localiser une personne ou un véhicule [***]
- Élargir la description des lieux où le mandat peut être exécuté pour qu’elle inclue [***]
- Ajouter le pouvoir d’intercepter [***]
- Ajouter le pouvoir d’obtenir des images de personnes qui sont mentionnées dans le mandat ou qui se trouvent à des endroits mentionnés dans le mandat.
- Ajouter, à la condition portant sur la conservation, une période d’évaluation de [***] après laquelle

after which the collected information (other than information from [***] must be destroyed unless the stipulated conditions have been met (i.e. the information relates to a threat, a crime, or the capabilities, intentions, or activities of the foreign state).

- Inclusion of a new condition allowing the Service to create backups of collected intercepted information.
- In the [***] Warrant, adding a power to obtain information about [***]

[96] The *amici* raised no significant concerns about these changes. I agree that the proposed modifications are routine and raise no legal issues.

(2) Clarifying the scope of some powers

[97] The Service wishes to clarify that it has the lawful authority to [***] This would enable the Service to intercept [***] without having to [***]

[98] Neither of these two activities would require any amendment to the warrants or involve the use of any new powers.

[99] The Service also seeks to clarify its power to search [***] This is not, strictly speaking, a new power but the Service proposes that the locations where searches can be carried out be expanded to include, [***]

[100] Again, the *amici* raised no concerns in this area, and I see no legal issues arising from the proposed amendments.

(3) New powers or locations

[101] The Service seeks two powers that it has not previously sought for purposes of section 16 investigations—search of [***] and the search of [***] In both cases, the searches would be confined to [***]locations used by foreign persons***]

les informations recueillies (hormis celles qui proviennent [***] devront être détruites, sauf si les conditions précisées ont été respectées (c'est-à-dire que les informations ont trait à une menace, à un crime ou aux moyens, intentions ou activités de l'État étranger).

- Ajouter une condition permettant au Service de créer des copies de sauvegarde des informations recueillies dans le cadre d'interceptions.
- Dans le mandat sur [***] ajouter le pouvoir d'obtenir des informations sur [***]

[96] Les *amici* n'ont exprimé aucune préoccupation importante à propos de ces modifications. Je conviens qu'il s'agit de modifications de routine qui ne soulèvent aucune question juridique.

2) Précision de la portée de certains pouvoirs

[97] Le Service souhaite préciser qu'il a le droit [***] Cela lui permettrait d'intercepter [***] sans avoir à [***]

[98] Ni l'une ni l'autre activité n'exigerait de modification aux mandats ni n'impliquerait l'exercice d'un nouveau pouvoir.

[99] Le Service cherche aussi à préciser le pouvoir de fouiller [***]. À proprement parler, il ne s'agit pas d'un nouveau pouvoir, mais le Service propose d'allonger la liste des lieux où les fouilles peuvent être effectuées pour qu'elle comprenne, [***]

[100] Encore une fois, les *amici* n'avaient aucun problème à cet égard, et je ne constate aucune question juridique que soulèveraient les modifications proposées.

3) Nouveaux pouvoirs ou lieux

[101] Le Service cherche à obtenir deux pouvoirs qu'il n'a jamais demandés aux fins des enquêtes menées au titre de l'article 16 : fouiller [***] ainsi que [***] Dans les deux cas, les fouilles seraient limitées aux [***]emplacements utilisés par des personnes étrangères***]

[102] These kinds of powers are frequently used in the section 12 context, and there is no obvious reason not to permit them for section 16 investigations.

(4) Conclusion on warrant templates

[103] Many of the amendments described above have been the subject of submissions and discussions with the Court following the *en banc* hearing giving rise to Justice Simon Noël's decision in the *Associated Data* case (*X (Re)*, 2016 FC 1105, [2017] 2 F.C.R. 396 [cited above]). These discussions are ongoing. Any changes or improvements to the wording of the section 12 warrant templates should generally result in corresponding changes to the warrant templates applicable in the foreign intelligence context.

III. Issue Two—Does section 16 authorize use of CSS technology?

[104] The Service seeks to confirm that its authority pursuant to section 16 of the CSIS Act includes the ability to capture information through use of cellular site simulators (CSS). CSS can be used to obtain data emitted by mobile devices, namely IMSI (International Mobile Security Identity) and IMEI (International Mobile Equipment Identity). The former reveals the country where the user's cellular account is located, the network code for the service provider, and a subscriber identity number assigned by the service provider. The latter indicates the make, model, and serial number of the device. No other attributes of targeted devices are captured through use of CSS. Nor is any content of communications captured. The sole purpose of CSS is to obtain information that could later be used in an application to the Court for a warrant to intercept the user's communications.

[105] This Court, in a decision authored by Chief Justice Paul Crampton, has addressed the use of CSS in the context of section 12 of the Act, that is, for purposes

[102] Les pouvoirs de ce genre sont fréquemment exercés dans le contexte de l'article 12, et il n'existe pas de motifs évidents de ne pas les accorder pour ce qui est des enquêtes relatives à l'article 16.

4) Conclusion au sujet des modèles de mandats

[103] Nombre des modifications susmentionnées ont fait l'objet d'observations et de discussions avec la Cour, par suite de l'audience tenue en séance plénière ayant donné lieu à la décision *Données connexes* du juge Simon Noël (*X (Re)*, 2016 CF 1105, [2017] 2 R.C.F. 396 [précitée]). Ces discussions ne sont pas terminées. En règle générale, tout changement ou toute amélioration au libellé des modèles de mandats relatifs à l'article 12 devrait entraîner des modifications correspondantes dans les modèles de mandats applicables au renseignement étranger.

III. Deuxième question — L'article 16 autorise-t-il le recours aux ESB?

[104] Le Service cherche à confirmer que ses pouvoirs au titre de l'article 16 de la Loi sur le SCRS comprennent la capacité de capturer des informations au moyen d'éémulateurs de station de base (ESB). Les ESB peuvent permettre d'obtenir des données émises par des appareils mobiles, à savoir l'identité internationale d'abonnement mobile (*International Mobile Subscriber Identity*) (IMSI), qui révèle le pays où est enregistré le compte d'utilisateur de l'appareil, le code de réseau du fournisseur de services et un numéro d'identification de l'abonné attribué par le fournisseur de service, ainsi que l'identité internationale d'équipement mobile (*International Mobile Equipment Identity*) (IMEI), qui précise la marque, le modèle et le numéro de série de l'appareil. Les ESB ne permettent d'obtenir aucune autre caractéristique des appareils visés, ni le contenu des communications. Les ESB ont une seule utilité : obtenir des informations susceptibles d'être utilisées dans une demande de mandats faite à la Cour en vue d'intercepter les communications de l'utilisateur.

[105] Sous la plume du juge en chef Paul Crampton, la Cour a traité du recours aux ESB dans le contexte de l'article 12 de la Loi sur le SCRS, c'est-à-dire aux

of investigating threats to national security (*X (Re)*, 2017 FC 1047, [2018] 3 F.C.R. 111 [*X (Re) (CSS)*]). The Chief Justice concluded that the use of CSS amounted to a search because users of mobile devices had a reasonable expectation of privacy in respect of the information CSS technology could capture. However, he found that use of CSS without a warrant was lawful so long as the Service took measures to minimize the intrusion on privacy by refraining from intercepting communications or information stored on the device, destroying any information collected incidentally from third parties, and desisting from using the information for purposes of geo-location. While the information available through CSS could assist the Service to create a thin personal profile of the user, thereby engaging section 8 of the Charter [*Canadian Charter of Rights and Freedoms*], the Chief Justice found that the warrantless searches were not unreasonable given that they were narrowly targeted, highly accurate, and minimally intrusive.

[106] The question before me is whether the analysis carried out by the Chief Justice in the national security context applies equally or, at least, comparably in the context of foreign intelligence gathering. At several points, the Chief Justice emphasized the special nature and purpose of section 12 of the Act, in particular, the state interest in obtaining information that would further its duty to protect national security. As discussed, the nature and purpose of section 16 differs from that of section 12. Does that difference affect the lawfulness of the Service's use of CSS technology without a warrant? To answer that question, I will review those parts of the Chief Justice's decision where the differences between the nature and purposes of section 16 and section 12 may influence the analysis. I will then consider other differences between the two provisions.

[107] The Chief Justice began by making clear that warrantless searches are presumptively unreasonable and contrary to the protection in section 8 of the Charter against unreasonable searches and seizures. Nevertheless, a search could be found to be reasonable if it was authorized by law, the law was reasonable, and the

fins d'enquêtes sur des menaces pour la sécurité nationale (*X (Re)*, 2017 CF 1047, [2018] 3 R.C.F. 111 [*X (Re) (ESB)*]). Le juge en chef a conclu que l'utilisation d'un ESB était assimilable à une fouille, parce que l'utilisateur d'un appareil mobile avait une attente raisonnable en matière de vie privée relativement aux informations qu'un ESB pourrait capturer. Toutefois, il a conclu à la légalité de l'utilisation d'un ESB sans mandat, tant que le Service prenait des mesures pour minimiser l'empiètement sur la vie privée, notamment éviter d'intercepter le contenu de communications et les informations stockés sur l'appareil, détruire toute information de tiers recueillie de manière incidente et ne pas utiliser les informations à des fins de géolocalisation. Bien que les informations que l'ESB permet d'obtenir puissent aider le Service à créer un mince profil personnel de l'utilisateur, ce qui met en cause l'article 8 de la *Charte canadienne des droits et libertés* (Charte), le juge en chef a conclu que les fouilles sans mandat n'étaient pas abusives, étant très ciblées, très précises et minimalement envahissantes.

[106] Je suis donc saisi de la question suivante : l'analyse effectuée par le juge en chef dans le contexte de la sécurité nationale tient-elle autant la route en matière de collecte de renseignements étrangers ou, du moins, y a-t-il des points de comparaison? Le juge en chef a insisté à plusieurs reprises sur la nature spéciale et sur l'objet de l'article 12 de la Loi sur le SCRS, en particulier sur l'intérêt de l'État envers l'obtention d'informations qui l'aideraient à assurer la sécurité nationale. Comme il en a été question, la nature et l'objet de l'article 16 sont différents. Cette différence a-t-elle une incidence sur la légalité du recours aux ESB sans mandat par le Service? Pour répondre à cette question, je vais examiner les parties de la décision du juge en chef où son analyse pourrait être influencée par les différences entre la nature et l'objet des articles 12 et 16. Je me pencherai ensuite sur d'autres différences entre ces deux dispositions.

[107] D'entrée de jeu, le juge en chef a clairement souligné que les fouilles effectuées sans mandat sont présumées abusives et contreviennent donc à la protection contre les fouilles, les perquisitions et les saisies abusives garantie par l'article 8 de la Charte. Néanmoins, une telle fouille pourrait être jugée non abusive si elle

search was executed reasonably. He found that, under section 12, the Service had an obligation to collect, analyze, and retain information and intelligence about activities posing a threat to national security (paragraph 196). The Act also sets out the circumstances when the Service should obtain a warrant (section 21). However, the Act does not require the Service to obtain a warrant whenever it seeks to gather information relating to national security even when a person's reasonable expectation of privacy is at stake. He found that there is a range of minimally intrusive activities the Service can carry out within its national security mandate without having to obtain a warrant (paragraph 198), again, so long as the law authorizes those activities, the law is reasonable, and the means of carrying out the search are reasonable.

[108] By contrast, under section 16, the Service may (not shall) assist the respective ministers in collecting foreign intelligence; its mandate is neither as strong nor as direct as its national security role. As is the case with section 12, though, the Service can pursue its section 16 mandate by applying for a warrant under section 21. Still, while the differences between the two statutory mandates are clear, there is no basis for finding that the requirements for a warrant differ on that ground alone. Just as the Service can collect some forms of information relating to national security under section 12 without having to obtain a warrant, so, too, can it assist in gathering some forms of foreign intelligence without a warrant. The Act provides the Service the authority to collect both kinds of information and intelligence. The requirement for a warrant is not engaged for all intrusions into reasonable expectations of privacy, only in respect of searches that would otherwise be unreasonable, as the Chief Justice found in respect of section 12 (paragraph 199). I find that minimally intrusive searches are authorized by section 16 without the requirement of a warrant.

est autorisée par une loi, si la disposition législative l'autorisant est raisonnable et si elle n'a pas été effectuée de manière abusive. Il a conclu qu'en vertu de l'article 12, le Service est tenu de recueillir, d'analyser et de conserver des informations et des renseignements sur des activités qui constituent des menaces pour la sécurité nationale (au paragraphe 196). En outre, l'article 21 de Loi sur le SCRS établit les circonstances entourant l'obtention d'un mandat par le Service. Par contre, la Loi sur le SCRS n'exige pas que le Service obtienne un mandat chaque fois qu'il cherche à recueillir des informations ayant trait à la sécurité nationale, même quand la collecte met en cause l'attente raisonnable d'une personne eu égard à sa vie privée. Il a constaté l'existence d'une gamme d'activités minimalement envahissantes que peut mener le Service pour assumer son rôle en matière de sécurité nationale sans devoir obtenir de mandat (au paragraphe 198), encore une fois, tant qu'elles sont autorisées par une loi, que la disposition législative les autorisant est raisonnable et que les fouilles ainsi effectuées ne le sont pas de manière abusive.

[108] À l'inverse, en vertu de l'article 16, le Service a la possibilité — mais pas l'obligation — de prêter son assistance aux ministres mentionnés à la collecte de renseignements étrangers. Il ne s'agit pas d'un rôle aussi prépondérant ni aussi direct que son rôle en matière de sécurité nationale. Par contre, en l'occurrence tout comme pour ce qui a trait à l'article 12, le Service peut faire une demande de mandats en vertu de l'article 21 pour s'acquitter de ses fonctions. Néanmoins, bien que les différences entre les deux rôles confiés au Service par sa loi habilitante soient claires, rien ne permet de conclure pour ce seul motif que les exigences relatives aux mandats sont différentes. Tout comme il peut recueillir sans mandat certaines informations relatives à la sécurité nationale en vertu de l'article 12, il peut prêter son assistance à la collecte de certains renseignements étrangers sans devoir obtenir de mandat. La Loi sur le SCRS l'autorise à recueillir les deux types d'informations et de renseignements. Les cas d'empiètement sur l'attente raisonnable en matière de vie privée n'exigent pas tous l'obtention d'un mandat; ce n'est le cas que des fouilles qui, autrement, seraient abusives, comme le juge en chef l'a conclu eu égard à l'article 12 (au paragraphe 199). Je conclus que l'article 16 autorise

[109] The Chief Justice found that section 12 was a reasonable law, considering its nature and purpose, the degree of intrusiveness it authorizes, the mechanism of intrusion, the availability of judicial supervision, and other checks and balances. The first of these criteria, the nature and purpose of the applicable statutory provision, differs significantly as between sections 12 and 16, as discussed above.

[110] The Chief Justice considered the nature and purpose of section 12 to be the assignment of responsibility to the Service, where strictly necessary, to collect, analyze, and retain information and intelligence in respect of activities it reasonably suspects constitute a “[threat] to national security”, a statutorily defined term (section 2). He described [at paragraph 203] this role as “critical, central and arguably essential”. He rejected arguments of the amici before him that the reasonable suspicion standard was unconstitutionally low, noting that that standard had been approved by the Supreme Court of Canada in cases where privacy interests were limited, important public interests were at stake, or the search method involved was highly accurate (paragraphs 206–207). Each of those circumstances, he concluded, was present in respect of searches using CSS for section 12 purposes—minimal intrusion, pressing national security concerns, and high precision.

[111] There are at least three notable differences in the nature and purpose of section 16 as compared to section 12. First, the role given to the Service under section 16 is permissive, not mandatory; the Service “may” assist the named ministers in the collection of information and intelligence relating to foreign persons or states. Realistically, however, given that the provision requires a personal request in writing of the Minister of National Defence or the Minister of Foreign Affairs, and the personal consent in writing of the Minister of Public Safety

la réalisation, sans mandat, de fouilles minimalement envahissantes.

[109] Le juge en chef a conclu au caractère raisonnable de l'article 12, compte tenu de sa nature et de son objet, de l'ampleur de l'intrusion qu'il autorise, du mécanisme d'intrusion qu'il permet d'utiliser, de la supervision judiciaire qu'il prévoit ainsi que d'autres mesures de contrôle. Comme il en est question plus haut, les premiers de ces éléments, c'est-à-dire la nature et l'objet de la disposition, diffèrent de façon importante entre les articles 12 et 16.

[110] Selon le juge en chef, la nature et l'objet de l'article 12 consistent en l'octroi, au Service, de la responsabilité de recueillir, d'analyser et de conserver, dans la mesure strictement nécessaire, des informations et des renseignements sur des activités pour lesquelles le Service a des motifs raisonnables de croire qu'elles constituent des « menaces envers la sécurité du Canada », au sens de l'article 2 de la Loi sur le SCRS. Il s'agit, selon le juge en chef, d'un rôle « central et, sans doute, essentiel » [au paragraphe 203]. Il a rejeté les arguments des *amici*, qui estimaient que le critère des motifs raisonnables de soupçonner était faible sur le plan constitutionnel, soulignant que ce critère avait été approuvé par la Cour suprême dans des affaires où le droit au respect de la vie privée était réduit, qui mettaient en cause des intérêts publics de premier plan ou qui traitaient de méthodes de fouilles très précises (aux paragraphes 206 et 207). Il a conclu que les fouilles réalisées au moyen d'ESB pour l'application de l'article 12 comportaient chacun de ces éléments : intrusion minimale, préoccupations urgente liées à la sécurité nationale et très grande précision.

[111] Il existe au moins trois grandes différences entre la nature et l'objet des articles 12 et 16. D'abord, l'article 16 donne au Service une autorisation; il ne lui impose pas une contrainte. En effet, le Service « peut » prêter son assistance au ministre de la Défense nationale ou des Affaires étrangères à la collecte d'informations et de renseignements sur des étrangers ou des États étrangers. Par contre, en pratique, il est difficile d'envisager une situation où le Service refuserait de prêter l'assistance demandée, dans la mesure où cette disposition

and Emergency Preparedness, it is difficult to conceive of a situation where the Service would decline to provide assistance on request.

[112] Second, the Service's section 16 mandate is not a direct responsibility to collect intelligence. The Service's role is to assist the named ministers; its role cannot be described as "critical, central and arguably essential". As Justice Noel has noted, section 16 has an "assistance or policy oriented goal, rather than a threat related one" (*X (Re)*, 2018 FC 738, [2019] 1 F.C.R. 567 [cited above], at paragraph 54). However, it is, no doubt, an important mandate and one which the ministers likely consider to be highly valuable to the discharge of their functions. But it is not on the same scale as the Service's s 12 core mandate to investigate threats to national security. As discussed, the Service's foreign intelligence role has always been seen as, at most, secondary to its national security mandate.

[113] Third, section 16 does not require that the collection of the information or intelligence be "strictly necessary" or set out a standard comparable to the "reasonable suspicion" threshold. Nor is there any statutory definition of the "capabilities, intentions or activities" of foreign entities that would limit the scope of the Service's inquiries. The Service's section 16 role is inherently broader than its section 12 mandate.

[114] Again, while the mandate given to the Service under section 16 differs in important ways from its section 12 role, that is not the equivalent of stating that the nature and purpose of section 16 is somehow less important or less vital to Canada's interests than those animating section 12. In section 16, Parliament envisioned the Service playing a significant role, albeit secondary to its section 12 mandate, in furthering Canada's interests in national defence and international affairs. Canada's capacities to defend itself and to conduct productive relations with other states are arguably as essential to its sovereignty as its ability to combat threats to its security.

exige que le ministre présente une demande écrite et que le ministre de la Sécurité publique et de la Protection civile donne son consentement personnel par écrit.

[112] Ensuite, l'article 16 ne charge pas directement le Service de recueillir des renseignements. Le rôle du Service, qui est de prêter son assistance aux ministres mentionnés, ne saurait être décrit comme « central et, sans doute, essentiel ». Comme l'a souligné le juge Noël, « l'article 16 comporte un objectif orienté vers l'assistance ou les politiques, plutôt que sur la menace » (*X (Re)*, 2018 CF 738, [2019] 1 R.C.F. 567 [précitée], au paragraphe 54). Par contre, il s'agit indubitablement d'une responsabilité importante que les ministres considèrent probablement comme très utile dans l'exercice de leurs fonctions, mais qui n'est pas de même calibre que le rôle fondamental confié au Service par l'article 12 : enquêter sur les menaces pour la sécurité nationale. Comme il en a été question, le rôle du Service en matière de renseignement étranger a toujours été secondaire, tout au plus, par rapport à son mandat eu égard à la sécurité nationale.

[113] Enfin, l'article 16 n'exige pas que la collecte d'informations ou de renseignement se fasse « dans la mesure strictement nécessaire » ni n'établit un critère comparable à celui des « motifs raisonnables de soupçonner ». En outre, aucune définition légale des termes « moyens, [...] intentions ou [...] activités » d'entités étrangères ne vient limiter la portée des enquêtes du Service. En soi, l'article 16 donne au Service un mandat plus large que l'article 12.

[114] Encore une fois, souligner les différences importantes entre les rôles que confèrent au Service les articles 12 et 16 ne revient pas à affirmer que la nature et l'objet de l'article 16 sont, en quelque sorte, moins importants ou cruciaux pour les intérêts du Canada que ceux de l'article 12. Au moyen de l'article 16, le législateur a prévu que le Service assume un rôle important, bien que secondaire, par rapport aux responsabilités prévues à l'article 12, en vue de faire progresser les intérêts du Canada en matière de défense nationale et d'affaires internationales. Il est possible de soutenir que la capacité du Canada de se défendre et d'entretenir des relations

[115] The amici argue that this last factor, particularly the absence of a reasonable suspicion standard, sets section 16 apart from section 12 in this context. In their view, to pass constitutional muster, a reasonable suspicion standard would have to be read into section 16; that is, the Service would be entitled to use CSS technology pursuant to section 16 only where it had reasonable grounds to suspect that a foreign person possessed information relating to the capabilities, intentions, or activities of a foreign state that would assist the Minister in the conduct of Canada's international affairs or national defence.

[116] I disagree. The absence of a reasonable suspicion threshold is not constitutionally fatal. Section 16 contains other requirements that, in this context, provide an adequate substitute for the reasonable suspicion standard. The Service can gather foreign intelligence only if the Minister of Foreign Affairs or the Minister of National Defence makes a personal written request for assistance and the Minister of Public Safety and Emergency Preparedness responds with a personal written consent. The Service acts only after two senior ministers of the Crown have concluded that the collection of foreign intelligence is required to protect Canada's interests in international affairs or defence. It falls to these ministers to determine the appropriateness of tasking the Service to execute its foreign intelligence mandate. I have no basis for questioning the *bona fides* of the ministers or doubting their capacity to determine what is in the best interests of Canada. In addition, of course, if the Service later seeks to employ more intrusive powers, the Court retains a discretion in respect of the issuance of warrants under section 21.

[117] Further, in practical terms, it is unlikely that the Service, acting pursuant to its foreign intelligence mandate, would expend scarce resources in trying to collect information from persons who are unlikely to

productives avec d'autres pays est aussi essentielle à sa souveraineté que sa capacité de lutter contre les menaces pour sa sécurité.

[115] Les *amici* soutiennent que ce dernier facteur, en particulier l'absence de critère relatif aux « motifs raisonnables de soupçonner », distingue l'article 16 de l'article 12 dans ce contexte. À leur avis, l'article 16 ne saurait résister à un examen constitutionnel sans qu'un tel critère y soit jugé implicite, c'est-à-dire que le Service pourrait utiliser les ESB uniquement s'il existe des motifs raisonnables de soupçonner qu'un étranger possède des informations sur les moyens, les intentions ou les activités d'un État étranger qui aideraient le ministre dans les domaines de la défense ou de la conduite des affaires internationales du Canada.

[116] Je ne suis pas d'accord. L'absence de critère relatif aux « motifs raisonnables de soupçonner » n'est pas fatale sur le plan constitutionnel. L'article 16 comporte d'autres exigences qui, dans ce contexte, constituent une solution de rechange adéquate au critère. Le Service ne peut recueillir des renseignements étrangers que si le ministre des Affaires étrangères ou de la Défense nationale présente lui demande personnellement, par écrit, de lui prêter son assistance, et que le ministre de la Sécurité publique et de la Protection civile donne son aval par écrit. Le Service n'agit qu'après que deux des principaux ministres fédéraux ont conclu que la collecte de renseignements étrangers est nécessaire pour protéger les intérêts du Canada en matière de défense ou d'affaires internationales. Il incombe à ces ministres de déterminer s'il est nécessaire de demander au Service de s'acquitter de son mandat eu égard au renseignement étranger. Rien ne me permet de remettre en question la bonne foi des ministres ni de douter de leur capacité à déterminer ce qui relève de l'intérêt supérieur du Canada. En outre, bien sûr, la Cour conserve son pouvoir discrétionnaire quant à la délivrance de mandats en vertu de l'article 21 si le Service cherche, plus tard, à exercer des pouvoirs envahissants.

[117] De plus, en pratique, il est peu probable que le Service, dans son rôle relatif au renseignement étranger, étire des ressources déjà rares pour tenter de recueillir des informations auprès de personnes qui ne savent

have knowledge of a foreign state's capabilities, intentions, or activities. In this way, section 16 is somewhat self-limiting, given that foreign intelligence gathering is not at the core of the Service's *raison d'être*. This distinguishes it from the Service's role under section 12, which is critical, central, and arguably essential. It is far more likely that the Service would be inclined to overreach in executing its section 12 mandate than in its section 16 role.

[118] In my view, there exist sufficient safeguards constraining the potential over-extension of the Service's foreign intelligence role to satisfy section 8 of the Charter in respect of minimally intrusive searches, such as the use of CSS, without a warrant.

[119] Therefore, in this context, I do not see a significant difference between the nature and purpose of section 16 as compared to section 12. In both areas, the Service's role furthers pressing national interests.

[120] In addition, though section 16 may lack the limiting language of section 12, it contains an essential constraint that does not apply to section 12—section 16 targets only foreign persons and states, not Canadians. Section 16's scope is broad; its application narrow.

[121] Parliament has recognized that the Service should have greater leeway in collecting information and intelligence about foreign entities in Canada for defence and international relations purposes than in investigating threats to the security of Canada.

[122] The point to be taken from the limits in section 16 is that they constrict the Service's powers in a manner consistent with its mandate to assist in protecting Canada's national defence and furthering its international relations. There are clear limits on the Service's authority under section 16 to execute minimally intrusive powers, such as the collection of data through CSS technology.

probablement rien des moyens, des intentions ou des activités d'un État étranger. En cela, l'article 16 constitue en quelque sorte sa propre limite, compte tenu du fait que la collecte de renseignements étrangers n'est pas au cœur de la raison d'être du Service, par rapport au rôle que lui confie l'article 12, qui est critique, central et, sans doute, essentiel. Il est bien plus probable que le Service soit enclin à trop en faire dans l'exécution de ce mandat qu'en ce qui concerne son rôle au titre de l'article 16.

[118] J'estime qu'il existe suffisamment de mécanismes permettant d'empêcher le Service d'aller trop loin dans son rôle eu égard au renseignement étranger pour que soit respecté l'article 8 de la Charte quant aux fouilles minimalement envahissantes menées sans mandat, comme l'utilisation d'ESB.

[119] Partant, dans ce contexte, je ne constate aucune différence importante entre les articles 12 et 16 en ce qui a trait à la nature et à l'objet. Dans les deux domaines, le rôle du Service sert les intérêts nationaux.

[120] En outre, bien qu'il ne comporte pas le libellé limitatif de l'article 12, l'article 16 comporte une contrainte essentielle à laquelle échappe l'article 12 : seuls des étrangers et des États étrangers peuvent être visés; les cibles ne peuvent pas être des Canadiens. L'article 16 a une portée large, mais un champ d'application étroit.

[121] Le législateur a reconnu que le Service devait avoir une latitude supérieure dans sa collecte d'informations et de renseignements sur les entités étrangères au Canada, à des fins de défense et de relations internationales, que celle dont il dispose pour enquêter sur les menaces pour la sécurité nationale.

[122] Il faut comprendre que les limites prévues à l'article 16 restreignent les pouvoirs du Service en fonction du rôle qui lui est confié, c'est-à-dire prêter son assistance en matière de défense nationale et d'avancement des relations internationales du Canada. Il existe des limites claires quant à l'exercice par le Service, au titre de l'article 16, de pouvoirs minimalement envahissants, comme la collecte de données au moyen d'ESB.

[123] The final factor to consider in respect of section 8 of the Charter is whether the search carried out—a CSS operation—is conducted in a reasonable manner. Chief Justice Crampton concluded, in the section 12 context, that the search was, indeed, reasonable. He considered the following factors:

- IMSI and IMEI captured from third parties was deleted or destroyed before any analysis of it was done;
- CSS operations have no discernible impact on the target's use of a device; in particular, CSS activities do not cause the user to drop calls, or prevent users from placing a 911 call; and
- CSS equipment cannot intercept the content of communications or capture information stored on a device (at paragraphs 238–242).

[124] The same factors exist for CSS operations conducted pursuant to section 16. I agree with the Chief Justice that the manner in which CSS operations are conducted is reasonable.

[125] Accordingly, I find no conflict between the warrantless use of CSS and section 8 of the Charter. Section 16 provides a sufficient and reasonable statutory basis for warrantless searches, so long as they are minimally intrusive and conducted in a reasonable manner.

IV. Issue Three—Does section 16 authorize interception of [***] data?

[***]The redactions in the following section concern technology that allows the Service to collect certain information from mobile devices. The Court concludes that the Service may use this technology, without a warrant, to obtain a specific subset of that information to identify that device for future purposes. However, the Court notes that the technology also allows the Service to acquire information from mobile devices that might permit the Service to learn about an individual's private

[123] Le dernier facteur à prendre en considération eu égard à l'article 8 de la Charte est le caractère raisonnable de l'exécution de la fouille — le recours à un ESB. Le juge en chef Crampton a conclu que, dans le contexte de l'article 12, elle était effectivement raisonnable. Il a pris en considération les facteurs suivants :

- Les IMSI et les IMEI de tiers recueillies ont été détruites avant de faire l'objet de la moindre analyse.
- Les opérations fondées sur des ESB ne nuisent d'aucune manière perceptible à l'expérience de l'utilisateur d'un appareil. En particulier, elles n'interrompent pas d'appels actifs ni n'empêchent l'utilisateur de composer le 911.
- Les ESB et le matériel connexe ne permettent pas d'intercepter le contenu d'une communication ou d'obtenir des informations stockées dans un appareil (aux paragraphes 238 à 242).

[124] Les mêmes facteurs s'appliquent aux opérations fondées sur des ESB menées au titre de l'article 16. Je conviens avec le juge en chef que les opérations fondées sur des ESB sont menées de manière raisonnable.

[125] Partant, je ne constate aucun conflit entre l'utilisation d'ESB sans mandat et l'article 8 de la Charte. L'article 16 offre un fondement légal suffisant et raisonnable aux fouilles sans mandat, pourvu qu'elles soient minimalement envahissantes et effectuées de manière raisonnable.

IV. Troisième question — L'article 16 autorise-t-il l'interception de données [***] ?

[***]Les caviardages dans la section ci-dessous concernent une technologie qui permet au Service de recueillir certaines informations d'un appareil portable. La Cour a conclu que le Service peut utiliser cette technologie sans mandat pour obtenir un sous-ensemble précis de ces informations afin d'identifier cet appareil à des fins futures. Toutefois, la Cour a soulevé le fait que la technologie pourrait aussi permettre au Service d'acquérir, à partir de l'appareil portable, des informations sur les

activities and personal choices. The Court holds that the Service requires a warrant to use the technology to acquire this further information.***]

[126] The Service submits that the interception of [***] data is essentially akin to CSS operations in that both are minimally intrusive searches conducted pursuant to valid and reasonable statutory authority (section 16) and are carried out in a reasonable manner.

[127] I disagree. Interceptions of [***] data capture more personal information than CSS operations. They require a warrant.

[128] I will first describe the technology relating to [***] interceptions and the information that can be retrieved with it. I will then consider whether section 16 provides sufficient authority for those interceptions or whether a warrant is required.

[129] The Service and the *amici* agree that [***] surveys do not contravene the *Radiocommunication Act* (R.S.C., 1985, c. R-2, paragraph 9(1)(b)) or the *Criminal Code* (R.S.C., 1985, c. C-46, sections 184, 430(1.1)(c)). I concur with their submissions and need not say anything further on that point. I note that Chief Justice Crampton came to a similar conclusion in respect of CSS operations (*(X (Re) (CSS)*, above, at paragraphs 82–106).

(1) The Technology

[130] The following overview is taken largely from the affidavit and testimony of [***] a Service employee with expertise in the area of [***]

[131] [***]

[132] [***]

[133] [***]

[134] [***]

activités privées ainsi que les choix personnels d'un individu. La Cour statue qu'un mandat est nécessaire pour acquérir ces informations supplémentaires.***]

[126] Le Service soutient que l'interception de données [***] et les opérations fondées sur les ESB sont essentiellement de même nature, car il s'agit dans les deux cas de fouilles minimalement envahissantes menées de manière raisonnable au titre de pouvoirs légaux valides et raisonnables (article 16).

[127] Je ne suis pas d'accord. L'interception de données [***] permet d'obtenir davantage d'informations personnelles que les opérations fondées sur les ESB et nécessite un mandat.

[128] En premier lieu, je vais aborder la technologie relative aux interceptions [***] et aux informations que celles-ci permettent d'obtenir. Je vais ensuite me prononcer sur la possibilité que l'article 16 suffise à autoriser ces interceptions, ou si un mandat doit être obtenu.

[129] Le Service et les *amici* conviennent que les sondages [***] ne contreviennent pas à l'alinéa 9(1)b) de la *Loi sur la radiocommunication*, L.R.C. (1985), ch. R-2, ni à l'article 184 ni à l'alinéa 430(1.1)c) du *Code criminel*, L.R.C. (1985), ch. C-46. Je suis d'accord avec leurs observations et je n'ai rien à ajouter à ce propos. Je souligne que le juge en chef Crampton en est arrivé à une conclusion similaire quant aux opérations fondées sur des ESB (*(X (Re) (ESB)* [précitée], aux paragraphes 82 à 106).

1) Technologie

[130] L'aperçu ci-dessous s'inspire largement de l'affidavit et du témoignage de [***] employé du Service spécialiste [***]

[131] [***]

[132] [***]

[133] [***]

[134] [***]

[135] [***]

[136] The Service engages in what it calls “[***] surveys.” In a survey, the Service obtains [***] in an effort to identify a particular device used by a target of an investigation.

[137] A survey involves the use of a device specially configured to capture [***] This kind of device can be portable or stationary. In either case, they are passive; [***] They do not intercept the contents of any communication or any [***] activity—they simply collect [***] An analysis of [***] can permit the Service to identify the particular device that a target is using.

[138] [***]

[139] [***]

[140] According to Service policy, surveys last no longer than [***] If the [***] target’s device has not been identified within that period of time, all information collected in the survey will be destroyed. If the [***] target’s device has been identified, the Service will retain it.

[141] The object of [***] surveys is to determine the [***] devices used by targets of investigation. With [***] the Service, armed with a warrant, can then begin to intercept the target’s [***] As with the use of CSS, obtaining [***] enables the Service to seek the authority to conduct more intrusive searches armed with a warrant.

[142] The Service makes clear that the only unique, permanent, and identifiable information it obtains through [***] surveys are [***] However, that is not the only information that is gathered.

[143] The Service also obtains ancillary information [***] Ancillary information about devices includes [***] The Service retains this information if it relates to [***] In other words, if the Service obtains [***] for a target’s device, [***] and the ancillary information associated with the device will be retained.

[135] [***]

[136] Le Service effectue ce qu’il appelle des « sondages [***] » qui lui permettent d’obtenir [***] en vue de reconnaître celui qu’utilise la cible de l’enquête.

[137] Pour ce faire, il utilise un appareil spécialement configuré pour capter, [***] Qu’il soit portable ou stationnaire, l’appareil est passif [***] Il n’intercepte ni le contenu des communications ni l’activité [***] Il recueille simplement [***] L’analyse [***] peut permettre au Service de déterminer quel appareil utilise sa cible.

[138] [***]

[139] [***]

[140] Conformément aux politiques du Service, les sondages ne durent pas plus de [***] Il détruit toute information recueillie au cours du sondage s’il n’a pas réussi à obtenir [***] de l’appareil de la cible pendant cette période. Si le Service obtient [***] il la conserve.

[141] Les sondages [***] visent à recenser [***] d’appareils utilisés par des cibles d’enquête. Fort [***] et d’un mandat, le Service peut commencer à intercepter [***] de la cible [***] Tout comme pour l’utilisation d’un ESB, l’obtention [***] permet au Service de demander un mandat permettant d’effectuer des fouilles plus envahissantes.

[142] Le Service précise bien que les seules informations uniques, permanentes et reconnaissables qu’il obtient grâce aux sondages [***] sont [***] Il ne s’agit pas, cependant, des seules informations qu’il recueille.

[143] Le Service obtient aussi des informations connexes, [***] S’agissant d’un appareil, ce sont des détails comme [***] Le Service conserve ces informations si elles ont trait à [***] Autrement dit, si le Service obtient [***] de l’appareil d’une cible, il conserve [***] et les informations connexes liées à l’appareil.

[144] Ancillary information [***] includes [***] The Service's own survey devices also generate ancillary information [***] Most useful to the Service are [***] of the survey device which establish [***] when the survey was conducted.

[145] The Service maintains that the two most useful pieces of information it captures through surveys are [***] The target's [***] are obtained through [***] It is only [***] that are revealed, not the [***] However, some information, such as the target's [***] can sometimes be gleaned [***]

[146] The [***] will tell the Service, for example, [***] This may allow the Service to determine the target's [***] behaviour patterns." In addition, that information may support a warrant application by the Service authorizing it to intercept the target's [***] through particular means.

[147] For example, if the target's [***] reveals that he or she usually [***] this may allow the Service to make use of [***]

[148] [***]

- (2) Does section 16 provide sufficient legal authority?

[149] The Service submits that the most valuable information it obtains in support of its section 16 mandate often comes from the intercepted communications of those [***foreign persons***] who are associated with [***foreign states, groups of foreign states, or foreign corporations***] in respect of which the Service is currently assisting the Minister [***]

[150] To obtain a warrant to carry out these interceptions, the Service must present reasonable grounds to believe that [***a foreign person or persons***] will be sending or receiving communications over a particular [***] device that is owned or leased by them [***] Similar to the use of CSS technology, [***] surveys allow the Service to obtain the unique electronic identifiers

[144] S'agissant [***] les informations connexes sont notamment [***] Le dispositif qu'utilise le Service pour effectuer les sondages génère aussi des données connexes [***] Ces dernières sont les plus utiles pour le Service, car elles permettent d'établir [***] au moment du sondage.

[145] Le Service soutient que les deux informations les plus utiles obtenues lors des sondages sont [***] de la cible. Il obtient [***] grâce aux [***] Seuls [***] sont révélés; les informations n'incluent pas [***] Cependant, [***] parfois une source d'informations, comme [***] de la cible.

[146] La [***] apprendra au Service, par exemple, [***] ce qui peut lui permettre d'établir ses habitudes [***] Le Service peut aussi évoquer ces informations dans une demande de mandats qui l'autoriseront à intercepter [***] de la cible grâce à des méthodes particulières.

[147] À titre d'exemple, si [***] de la cible révèle [***] le Service pourrait se servir [***]

[148] [***]

- 2) L'article 16 constitue-t-il une autorisation légale suffisante?

[149] Le Service avance que, dans bien des cas, les informations les plus utiles qu'il recueille dans l'exercice du rôle que lui confie l'article 16 découlent des communications interceptées [***des personnes étrangères***] [***qui sont associées à des États étrangers, groupes d'États étrangers, ou personnes morales étrangères***] à propos desquels il prête actuellement son assistance au ministre [***]

[150] Pour obtenir un mandat lui permettant de procéder à ces interceptions, le Service doit donner des motifs raisonnables de croire [***qu'une personne, ou des personnes, étrangères***] effectueront ou recevront des communications au moyen [***] en particulier [***] dont eux-mêmes [***] sont propriétaires ou qu'ils louent. [***] À l'instar des ESB, les sondages [***] permettent

associated with the devices which, in turn, will permit the Service to conduct warranted interceptions [***]

[151] The Service concedes that the use of [***] surveys to obtain [***] amounts to a search for purposes of section 8 of the Charter. However, the Service maintains that these searches constitute a minimal intrusion on individuals' expectations of privacy. [***], according to the Service, is similar to the IMSI and IMEI information collected through CSS and no breach of section 8 takes place when the Service obtains that kind of information without a warrant. [***] reveals nothing about the user.

[152] In respect of [***], the Service contends that the information it obtains about a user's [***] is "often relatively weak and non-invasive." At most, it tells the Service [***]

[153] Further, the Service argues that section 16 provides reasonable lawful authority for conducting [***] surveys that generate [***] Parliament, says the Service, has explicitly authorized the Service under section 16 to collect foreign intelligence, within Canada, to assist the ministers of Foreign Affairs and Defence in determining the capabilities, intentions, or activities of foreign persons.

[154] The Service submits that section 16 complies with the requirement that the statutory basis for a warrantless search be transparent in its grant of official powers, and that it set out clear criteria (citing *R. v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212 [*Spencer*] and *R. v. Shoker*, 2006 SCC 44, [2006] 2 S.C.R. 399). In addition, the Service argues that section 16 does not establish an unconstitutionally vague standard (as described in *R. v. Nova Scotia Pharmaceutical Society*, [1992] 2 S.C.R. 606, (1992), 93 D.L.R. (4th) 36).

[155] In any case, says the Service, a low standard is appropriate in this context where privacy interests are reduced and state objectives predominate (*R. v. Chehil*, 2013 SCC 49, [2013] 3 S.C.R. 220, at paragraph 23; *X (Re) (CSS)*, above, at paragraph 206).

au Service d'obtenir les identifiants électroniques uniques ayant trait aux appareils, ce qui leur permet ensuite de procéder, en vertu de mandats, à l'interception [***]

[151] Le Service reconnaît que le recours aux sondages [***] pour obtenir [***] constitue une fouille visée à l'article 8 de la Charte. Il soutient toutefois que de telles fouilles constituent des atteintes minimales à l'attente des personnes au respect de leur vie privée. Le Service estime [***] est comparable à l'IMSI et à l'IMEI recueillis au moyen d'un ESB, c'est-à-dire qu'il s'agit d'une information dont la collecte sans mandat n'enfreint pas l'article 8. [***] ne révèle rien à propos de son utilisateur.

[152] En ce qui a trait [***] le Service soutient que les informations obtenues sur [***] l'utilisateur [TRADUCTION] « ont souvent une utilité relativement faible et sont peu indiscretes ». Tout au plus, elles révèlent au Service [***]

[153] En outre, le Service soutient que l'article 16 constitue une autorisation légale raisonnable de procéder aux sondages [***] qui lui permettent d'obtenir [***] Le Service estime que le législateur, au moyen de l'article 16, l'a explicitement autorisé à recueillir des renseignements étrangers, dans les limites du Canada, pour aider les ministres des Affaires étrangères et de la Défense à déterminer les moyens, les intentions et les activités d'étrangers.

[154] Selon le Service, l'article 16 respecte l'exigence selon laquelle la disposition législative qui autorise une fouille sans mandat doit clairement octroyer un pouvoir officiel et établir des critères limpides (citant *R. c. Spencer*, 2014 CSC 43, [2014] 2 R.C.S. 212 (*Spencer*) et *R. c. Shoker*, 2006 CSC 44, [2006] 2 R.C.S. 399). En outre, de l'avis du Service, l'article 16 n'établit pas un critère vague au point d'en être inconstitutionnel (comme en fait état l'arrêt *R. c. Nova Scotia Pharmaceutical Society*, [1992] 2 R.C.S. 606).

[155] Le Service ajoute que, de toute façon, l'application d'une norme moins rigoureuse se justifie dans un tel contexte, lorsque les droits à la vie privée sont réduits ou lorsque les objectifs de l'État sont prédominants (*R. c. Chehil*, 2013 CSC 49, [2013] 3 R.C.S. 220, au paragraphe 23; *X (Re) (ESB)*, au paragraphe 206).

[156] In addition, the Service points to a number of features of section 16 that it says are indicative of its reasonableness. These factors largely track the submissions the Service put forward in respect of CSS operations, discussed above, but bear repeating in this context.

(a) *Nature and Purpose:*

[157] Section 16 fulfills an important state purpose, namely, the collection of foreign intelligence to assist the ministers in relation to the defence of Canada and its international affairs.

(b) *Criteria and Limits:*

[158] The provision contains objective criteria and strict limits, notably, the requirements that a Minister request the Service's assistance in writing; that the Minister of Public Safety must personally consent to the assistance; that the assistance be connected to a foreign state's capabilities, intentions, or activities; that Canadians not be targeted; and that the assistance must take place within Canada.

(c) *Balance:*

[159] Section 16 strikes a balance between the public interest in the collection of foreign intelligence and personal privacy. The ministers must weigh these factors before initiating a request for assistance and engaging the Service's use of investigatory techniques.

(d) *Minimally Intrusive:*

[160] Since the Service can invoke the intrusive warranted powers under section 21 of the Act in pursuit of its section 16 mandate, it follows that section 16 allows for the collection of information through minimally intrusive means without a warrant.

[156] En outre, le Service souligne différentes caractéristiques de l'article 16 qui, à son avis, attestent de son caractère raisonnable. Ces facteurs concordent en gros avec les demandes présentées par le Service quant aux opérations fondées sur des ESB, dont il est question plus haut. Il est toutefois utile de les répéter ici.

a) *Nature et objet*

[157] L'article 16 permet d'atteindre un important objectif étatique, à savoir la collecte de renseignements étrangers en vue d'aider les ministres en matière de défense nationale et d'affaires internationales.

b) *Critères et limites*

[158] L'article 16 comporte des critères objectifs et prévoit des limites strictes, notamment les obligations suivantes : un ministre demande l'assistance du Service par écrit; le ministre de la Sécurité publique y consent personnellement; l'assistance porte sur les moyens, les intentions ou les activités d'un État étranger, ne peut viser aucun Canadien et est prêtée dans les limites du Canada.

c) *Équilibre*

[159] L'article 16 établit un équilibre entre, d'une part, l'intérêt public dans la collecte de renseignements étrangers et, d'autre part, le respect de la vie privée. Les ministres doivent mettre ces facteurs en balance avant de présenter une demande d'assistance qui amènera le Service à utiliser des techniques d'enquête.

d) *Empiètement minimal*

[160] Puisque le Service peut exercer des pouvoirs envahissants en vertu de mandats visés à l'article 21 de la Loi sur le SCRS pour assumer le rôle que lui confie l'article 16, il s'ensuit que l'article 16 permet la collecte d'informations sans mandat grâce à des méthodes minimalement envahissantes.

(e) *Accuracy:*

[161] The manner in which the Service conducts [***] surveys ensures that the information it collects accurately identifies the device being used by the target and filters out information relating to other devices.

(f) *Accountability:*

[162] The Service is accountable for its activities to the Minister of Public Safety and is bound by the Ministerial Direction for Operations and Accountability. In addition, the conduct of the Service was reviewed by the Security and Intelligence Review Committee (SIRC); it is now accountable to the National Security and Intelligence Agency (NSIRA).

[163] The Service also maintains that the other limits that section 12 contains—that collection is strictly necessary and that there exist reasonable grounds to suspect—are not appropriate in the section 16 context.

[164] The *amici* point out, however, that a warrantless search is presumptively unreasonable for purposes of section 8 of the Charter (*R. v. Collins*, [1987] 1 S.C.R. 265, (1987), 38 D.L.R. (4th) 508). To conform with section 8, a warrantless search must be expressly authorized by a reasonable law and be carried out reasonably. The *amici* assert that the searches that result from [***] surveys are not authorized by section 16 and the power to conduct them cannot be implied.

[165] The *amici* also contend that these searches are more than minimally intrusive and, therefore, that they can be conducted only pursuant to a warrant. In particular, these kinds of searches permit investigators to build personal profiles of targets [***]

[166] I have already found that section 16 provides a sufficient, reasonable statutory basis for conducting warrantless, minimally intrusive searches, namely, capturing IMSI and IMEI information through reasonably-conducted CSS operations. I find the same is true in respect of the use of

e) *Précision*

[161] La façon dont procède le Service pour effectuer des sondages [***] assure que les informations recueillies permettent de reconnaître l'appareil utilisé par la cible et que les informations liées à d'autres appareils sont laissées de côté.

f) *Reddition de comptes*

[162] Le Service rend compte de ses activités au ministre de la Sécurité publique et est assujéti aux instructions du ministre sur les opérations et la reddition de comptes. En outre, l'Office de surveillance des activités en matière de sécurité nationale et de renseignement examine la conduite du Service (cela revenait auparavant au CSARS).

[163] Le Service soutient également que les autres limites prévues à l'article 12 (collecte dans la mesure strictement nécessaire et existence de motifs raisonnables de soupçonner) ne s'appliquent pas dans le contexte de l'article 16.

[164] Cependant, les *amici* soulignent que, pour l'application de l'article 8 de la Charte, une fouille sans mandat est présumée abusive (*R. c. Collins*, [1987] 1 R.C.S. 265). Pour ne pas enfreindre l'article 8, une fouille sans mandat doit être autorisée expressément par une disposition législative raisonnable et être effectuée de façon raisonnable. Les *amici* soutiennent que l'article 16 n'autorise pas les fouilles que constituent les sondages [***] et que le pouvoir de les effectuer ne saurait être considéré comme implicite.

[165] À leur avis, ces fouilles sont plus que minimalement envahissantes et, partant, ne peuvent être effectuées qu'en vertu d'un mandat. Notamment, elles permettent aux enquêteurs d'établir le profil personnel de cibles [***]

[166] J'ai déjà conclu que l'article 16 offre un fondement légal suffisant et raisonnable aux fouilles sans mandat minimalement envahissantes, notamment l'obtention de l'IMSI et de l'IMEI au moyen d'opérations fondées sur des ESB menées de façon raisonnable. Ma

[***] surveys, as described above, to capture [***] of targets' devices. [***] reveals nothing personal about the target. It simply permits the Service to identify the device for future purposes. Essentially, [***] are analogous to IMSI and IMEI in the CSS context.

[167] Accordingly, I agree with the Service that section 16 provides a reasonable statutory basis for capturing [***] of targets' devices through [***] surveys.

[168] I am also satisfied that minimally intrusive [***] surveys conducted pursuant to section 16 are carried out reasonably. As with CSS technology, there is no impact on any private communications, [***] or other private information stored in the device. Any third-party information collected is destroyed.

[169] However, I come to a different conclusion regarding the other information the Service would obtain through [***] surveys—[***]

[170] Again, the Service concedes that [***] surveys are searches but argues that, as with CSS operations, these surveys are minimally intrusive and should not require a warrant.

[171] It is important to note, however, in respect of [***], the kind of search that is in issue here. The target of a search would have a strong interest in keeping their personal activities private, and have an obvious subjective expectation of privacy. That expectation would be reasonable in the circumstances.

[172] As described above, [***] may tell investigators about the target's private activities and allow inferences to be made about the person's personal choices. The significance of the information collected is an important factor to consider in this context (*R. v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212 [cited above], at paragraphs 18, 26–31; *R. v. A.M.*, 2008 SCC 19, [2008] 1 S.C.R. 569, at paragraph 38).

conclusion est la même eu égard au recours au sondage [***] dont il est question plus haut, qui servent à obtenir [***] des appareils des cibles. [***] ne révèle aucun renseignement personnel sur la cible. Elle permet simplement au Service de reconnaître l'appareil pour des motifs ultérieurs. Essentiellement, dans le contexte [***] est analogue à l'IMSI et à l'IMEI dans le contexte des ESB.

[167] Partant, je conviens avec le Service que l'article 16 offre un fondement légal raisonnable à l'obtention [***] des appareils d'une cible au moyen de sondages [***]

[168] En outre, je suis convaincu que les sondages [***] minimalement envahissants, menés au titre de l'article 16, le sont raisonnablement. Comme pour la technologie relative aux ESB, il n'y a aucune incidence sur les communications privées, [***] ou toute autre information privée stockée dans l'appareil. Les informations de tiers recueillies sont détruites.

[169] Cependant, j'en arrive à une conclusion différente en ce qui a trait aux autres informations que le Service obtiendrait au moyen des sondages [***]

[170] Je réitère que le Service reconnaît que les sondages [***] constituent des fouilles, mais soutient qu'à l'instar des opérations fondées sur les ESB, ces sondages sont minimalement envahissants et devraient pouvoir être effectués sans mandat.

[171] Par contre, en ce qui a trait [***] il est important de souligner le genre de fouille en cause. La cible d'une telle fouille aurait un intérêt considérable à garder privées ses activités personnelles, et elle a manifestement une attente subjective en matière de vie privée. Dans les circonstances, il s'agirait d'une attente raisonnable.

[172] Comme il en est question plus haut, [***] peuvent renseigner les enquêteurs sur les activités privées de la cible et leur permettre de tirer des conclusions quant à ses choix personnels. L'importance des informations recueillies est un facteur dont il faut tenir compte dans ce contexte (*Spencer*, aux paragraphes 18 et 26 à 31; *R. c. A.M.*, 2008 CSC 19, [2008] 1 R.C.S. 569, au paragraphe 38).

[173] In *Spencer*, Justice Thomas Cromwell, for the Court, underscored the need for a purposive approach to section 8 issues, one that seeks “the protection of privacy as a prerequisite to individual security, self-fulfilment and autonomy as well as to the maintenance of a thriving democratic society” (paragraph 15). In particular, in determining whether a person had a reasonable expectation of privacy, one must consider the totality of the circumstances and consider the subject matter of the search, the affected person’s interest in that subject matter, the person’s subjective expectation of privacy, and the reasonableness of that expectation (paragraph 18).

[174] With respect to the subject matter of the search, it is often important to look beyond the actual information that has been captured and consider what that information reveals. For example, in *Spencer*, Justice Cromwell found that the subject matter of the search went beyond the subscriber information that was obtained by the police and included the personal lifestyle details that could potentially be disclosed by that information (paragraphs 25, 26). In effect, it allowed the police to correlate a person’s name and address with activities that were of interest to state authorities; in that case, collection of child pornography. The subject matter of a search should not be defined narrowly (*R. v. Reeves*, 2018 SCC 56, [2018] 3 S.C.R. 531, at paragraph 29). This is particularly important when considering searches of electronic information (*R. v. Marakah*, 2017 SCC 59, [2017] 2 S.C.R. 608 [*Marakah*], at paragraph 14).

[175] Similarly, the Supreme Court has held that the information obtained when a police dog sniffs a package is simply the odour emanating from it; but the dog’s reaction to the smell permits an inference to be made about the contents of the package (see *R. v. Kang-Brown*, 2008 SCC 18, [2018] 1 S.C.R. 456 [*Kang-Brown*]). In determining the subject matter of a search, then, one must look beyond the information obtained to the inferences that could be drawn from it (*Marakah*, at paragraph 20).

[173] Dans l’arrêt *Spencer*, le juge Thomas Cromwell, au nom de la Cour, souligne la nécessité d’adopter une approche téléologique aux questions qui mettent en cause l’article 8, axée 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 » (au paragraphe 15). En particulier, pour déterminer si une personne a une attente raisonnable en matière de vie privée, il est nécessaire de prendre en considération l’ensemble des circonstances ainsi que l’objet de la recherche, le droit de la personne concernée à l’égard de l’objet, l’attente subjective de la personne en matière de respect de sa vie privée ainsi que le caractère raisonnable de cette attente (au paragraphe 18).

[174] En ce qui a trait à l’objet de la fouille, il est souvent important de voir au-delà des informations elles-mêmes et de tenir compte de ce qu’elles révèlent. À titre d’exemple, dans l’arrêt *Spencer*, le juge Cromwell a conclu que l’objet de la fouille allait au-delà des informations sur l’abonné obtenues par la police et touchait aussi aux détails sur le mode de vie que ces informations pourraient finir par révéler (aux paragraphes 25 et 26). En effet, elles ont permis aux policiers de mettre en rapport le nom et l’adresse d’une personne avec des activités auxquelles s’intéressaient les autorités étatiques, en l’occurrence la collecte de pornographie infantile. Il ne faut pas définir l’objet de la fouille de façon restrictive (*R. c. Reeves*, 2018 CSC 5, [2018] 3 R.C.S. 531, au paragraphe 29), particulièrement lorsqu’elle porte sur des données électroniques (*R. c. Marakah*, 2017 CSC 59, [2017] 2 R.C.S. 608 (*Marakah*), au paragraphe 14).

[175] De même, la Cour suprême a soutenu que les informations obtenues lorsqu’un chien renifle un colis sont, purement et simplement, les odeurs qui en émanent. Toutefois, la réaction du chien permet d’inférer le contenu du colis (*R. c. Kang-Brown*, 2008 CSC 18, [2018] 1 R.C.S. 456 [*Kang-Brown*]). Partant, pour déterminer l’objet d’une recherche, il est nécessaire d’aller au-delà des informations obtenues et de s’intéresser aux conclusions qu’il est possible d’en tirer (*Marakah*, au paragraphe 20).

[176] Here, information about a person's [***] would allow the Service to draw inferences about that person's lifestyle and private activities. Individuals would have a direct interest in that subject matter and would subjectively expect that information to be kept private.

[177] In my view, that subjective expectation of privacy would be reasonable in the circumstances. Particularly significant in this context is the private nature of the information that can be inferred [***] The Service rightly points out that [***] will often reveal nothing about the owner of a device. For example, [***] may simply be [***] On the other hand, however, [***] may disclose the [***] with which the person of interest can be associated—[***] Typically, owners of devices have no control over [***] except possibly [***] This absence of control, however, does not mean that their expectation of privacy in the information that can be revealed is not reasonable (*Marakah*, at paragraph 41).

[178] Therefore, in my view, the information [***] may allow inferences to be drawn about lifestyle choices and private activities that individuals would wish to maintain and shield from state authorities (*R. v. Plant*, [1993] 3 S.C.R. 281, at page 293, (1993), 145 A.R. 104). Their expectation of privacy in that information is reasonable.

[179] Accordingly, given this difference between CSS operations, which involve minimally intrusive collections, and [***] surveys, which may involve collection of intrusive lifestyle information, I find that the latter require a warrant. These surveys may result in the gathering of personal information that is not open to public view and not released or abandoned by the targets of investigations. These factors tend in the direction of requiring a warrant (*R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432, at paragraph 32).

[180] In addition, I have no evidence before me suggesting that it would be impracticable or infeasible to obtain a warrant to conduct [***] surveys (*Kang-Brown*, at paragraph 59).

[176] En l'espèce, [***] d'une personne permettrait au Service de tirer des conclusions quant à son mode de vie et à ses activités privées. Une personne aurait un intérêt direct en la matière et s'attendrait subjectivement à ce que ces informations demeurent du domaine privé.

[177] À mon avis, cette attente subjective en matière de vie privée serait raisonnable dans les circonstances. Le caractère privé des informations qui peuvent être inférées [***] revêt une importance particulière dans ce contexte. Le Service souligne à juste titre que, souvent, [***] ne révélera rien du propriétaire d'un appareil. À titre d'exemple, il peut s'agir d'une simple [***] En revanche, [***] peut révéler [***] la personne d'intérêt peut être liée, [***] En général, le propriétaire d'un appareil n'a aucun pouvoir sur [***] sauf peut-être [***] Cette absence de contrôle ne signifie cependant pas que l'attente en matière de vie privée eu égard aux informations susceptibles d'être révélées n'est pas raisonnable (*Marakah*, au paragraphe 41).

[178] Ainsi, à mon avis, les informations [***] peuvent permettre de tirer des conclusions sur des éléments du mode de vie et des activités privées de personnes qui souhaiterait les conserver et les mettre à l'abri des autorités étatiques (*R. c. Plant*, [1993] 3 R.C.S. 281, à la page 293). Leur attente en matière de respect de la vie privée eu égard à ces informations est raisonnable.

[179] Partant, compte tenu de la différence entre une opération fondée sur les ESB, qui implique une collecte minimalement envahissante, et le sondage [***] qui peut entraîner la collecte envahissante d'informations sur le mode de vie, je conclus que ce dernier nécessite un mandat. De tels sondages peuvent mener à la collecte de renseignements personnels à caractère privé, qui n'ont été ni divulgués ni abandonnés par la cible d'une enquête. Ces facteurs tendent à démontrer qu'un mandat est nécessaire (*R. c. Tessling*, 2004 CSC 67, [2004] 3 R.C.S. 432, au paragraphe 32).

[180] En outre, rien de ce que j'ai devant moi ne porte à croire qu'il serait impossible ou infaisable d'obtenir un mandat pour effectuer un sondage [***] (*Kang-Brown*, au paragraphe 59).

[181] While I found that section 16 is a reasonable law to the extent that it permits conducting minimally intrusive searches without a warrant, I cannot come to the same conclusion regarding [***] surveys that collect personal lifestyle information. In my view, impartial judicial prior authorization—a warrant—is required for the Service to collect that information. In essence, I agree with Chief Justice Crampton when he found that “once [the Service] moves beyond minimally invasive collection activities, it will require a warrant” (*X (Re) (CSS)*, at paragraph 219).

V. Issue Four—Does section 16 authorize interception of communications outside Canada?

[182] The Service seeks an assurance that it has lawful authority to intercept [***a foreign person’s***] communications from within Canada even if [***the foreign person***] is outside of Canada. The Service claims that this authority would enhance its ability to collect information relevant to the particular [***] capabilities, intentions, or activities.

[183] The issue arises because of the requirement in section 16 that foreign intelligence be collected only “within Canada”. The words “within Canada” have been the subject of other litigation in this Court, most particularly in the case of *X (Re)* ([***]), 2018 FC 738, [2019] 1 F.C.R. 567 [cited above], affd in *X (Re)* ([***]) 2018 FCA 207. There, Justice Simon Noël concluded that the words “within Canada” in section 16 unambiguously mean within Canada’s geographical boundaries (at paragraphs 62, 100).

[184] The *amici* agree with the Service that the geographical requirements of section 16 are met when interceptions take place within Canada in respect of communications outside Canada.

[185] I agree. Still, to make clear what the Service proposes, I describe how these interceptions occur.

[181] Si j’ai effectivement conclu que l’article 16 est une disposition législative raisonnable qui permet la réalisation de fouilles minimalement envahissantes sans mandat, je ne peux pas trancher de la même manière en ce qui a trait aux sondages [***] qui permettent de recueillir des renseignements personnels sur le mode de vie. À mon avis, le Service doit obtenir au préalable une autorisation judiciaire impartiale, c’est-à-dire un mandat, pour recueillir ces informations. Essentiellement, je suis donc d’accord avec le juge en chef Crampton lorsqu’il conclut « lorsqu’il passe à des activités de collecte plus envahissantes, le Service doit obtenir un mandat » (*X (Re) (ESB)*, au paragraphe 219).

V. Quatrième question — L’article 16 autorise-t-il l’interception de communications à l’extérieur du Canada?

[182] Le Service cherche à s’assurer qu’il a le pouvoir légitime d’intercepter les communications [***d’une personne étrangère***] dans les limites du Canada, même si [***cette personne étrangère***] se trouve à l’étranger. Le Service estime que ce pouvoir accroîtrait sa capacité de recueillir des informations sur les moyens, les intentions ou les activités [***] en cause.

[183] Cette question est soulevée parce qu’aux termes de l’article 16, les renseignements étrangers ne peuvent être recueillis que « dans les limites du Canada ». La Cour a été saisie d’autres litiges relatifs à l’expression « dans les limites du Canada », surtout dans la décision *X (Re)*, 2018 CF 738, [2019] 1 R.C.F. 567 [précitée] (dossier [***]), décision confirmée dans *X (Re)*, ([***]), 2018 CAF 207. Le juge Simon Noël y a conclu que l’expression « dans les limites du Canada » figurant à l’article 16 signifie, sans équivoque, dans les frontières géographiques du pays (aux paragraphes 62 et 100).

[184] Les *amici* conviennent avec le Service qu’il y a respect de la restriction géographique de l’article 16 lorsqu’il y a interception, dans les limites du Canada, de communications à l’étranger.

[185] Je suis d’accord. Néanmoins, pour qu’il n’y ait pas d’ambiguïté sur ce que le Service propose, je décris le déroulement de ces interceptions.

[186] A Service employee in charge of building software used in the collection of information from Communications Service Providers (CSPs), [***] explained how interceptions are made within Canada of communications outside Canada.

[187] The Service is able to conduct “telecom intercepts” of telephone communications, mobile device communications, and Internet activities [***]

[188] The Service refers to these interceptions as “Lawful Intercepts” or “LI” when conducted for purposes of protecting national security or assisting law enforcement pursuant to judicially-authorized warrants. [***]

[189] When a person leaves Canada, his or her phone will search for a suitable local service provider, one with which the person’s Canadian CSP has entered into an agreement. This is commonly called “roaming.” The foreign service provider will exchange information with the Canadian CSP in order to confirm that the person is a subscriber with a service plan.

[190] Accordingly, Canadian CSPs are aware when their customers leave the country and use their phones outside Canada. [***]

[191] [***]

[192] In the absence of clear legal authority permitting the Service to intercept a person’s communications outside of Canada, the Service’s current practice is to terminate an interception (their operation “goes down”) if it becomes aware that [***a foreign person***] has left Canada. However, if [***the foreign person***] has left the country without the Service being aware, the interceptions will continue.

[193] Based on this evidence, I am satisfied that the Service’s proposed interceptions will be made within Canada and will comply with the geographical limits of section 16. Essentially, the situation is analogous to domestic interceptions of foreign communications under section 12 as addressed comprehensively by Justice

[186] [***] employé du Service chargé de mettre au point un logiciel servant à la collecte d’informations auprès de fournisseurs de services de communication (FSC), a expliqué comment le Service intercepte, dans les limites du Canada, des communications à l’étranger.

[187] [***] le Service est en mesure d’intercepter des communications effectuées au moyen de téléphones et d’appareils mobiles ainsi que des activités Internet, [***]

[188] Selon le Service, il s’agit [TRADUCTION] d’« interceptions légales » [IL] lorsqu’elles sont menées en vue d’assurer la sécurité nationale ou d’aider à faire appliquer la loi en vertu de mandats judiciaires. [***]

[189] Le téléphone d’une personne qui se rend à l’étranger cherchera un fournisseur de service local adéquat, c’est-à-dire avec lequel le FSC canadien de la personne a conclu une entente. Ce processus est couramment appelé « itinérance ». Le fournisseur étranger échange des informations avec le FSC canadien afin de confirmer que la personne est bel et bien une abonnée disposant d’un forfait de services.

[190] En conséquence, le FSC canadien sait quand un client quitte le Canada et utilise son téléphone à l’étranger. [***]

[191] [***]

[192] Pour l’heure, puisqu’aucune disposition législative ne l’autorise clairement à intercepter les communications d’une personne à l’étranger, le Service a pour pratique de mettre fin à l’interception s’il apprend que [***la personne étrangère***] a quitté le Canada. L’interception se poursuivra cependant si [***la personne étrangère***] quitte le pays à l’insu du Service.

[193] Compte tenu de ces éléments de preuve, je suis convaincu que les interceptions que propose le Service auront lieu dans les limites du Canada et, partant, respecteront la restriction géographique prévue à l’article 16. Essentiellement, la situation est similaire aux interceptions, au Canada, de communications

Richard Mosley in *X (Re)*, 2009 FC 1058, [2010] 1 F.C.R. 460.

VI. Conclusion and Disposition

[194] This application provided an opportunity for the Court to receive from the Service detailed information about certain aspects of its foreign intelligence mandate under section 16 of the CSIS Act. In particular, the Service explained its policies and practices relating to the incidental collection of information about Canadians, including elected officials, and to the pursuit of parallel section 16/section 12 operations. In both of these areas, I found the Service's conduct generally to be appropriate and satisfactory. However, I suggest that the Service should develop guidelines for distributing and unminimizing the identities of Canadians whose communications have been incidentally intercepted, and should provide the Court an opportunity to comment on them. It should also specifically disclose when there is a possibility that the communications of an elected official or other public servant may be intercepted, allowing the Court to impose any necessary terms and conditions on the execution of the warrants. Those terms and conditions could include imposing a requirement on the Service to return to the Court for directions on the handling of information collected.

[195] I also agree with the Service's proposed amendments to its section 16 warrant templates.

[196] I conclude that section 16 provides sufficient legal authority for the Service to carry out minimally intrusive searches to collect foreign intelligence. Use of CSS technology in the manner proposed by the Service falls into this category of searches and, therefore, does not require a warrant.

[197] However, I find that the interception of [***] data, to the extent that it captures a person's [***] is more than minimally intrusive. Having access to an individual's [***] would allow the Service to draw

étrangères effectuées en vertu de l'article 12, dont le juge Richard Mosley a traité en détail dans la décision *X (Re)*, 2009 CF 1058, [2010] 1 R.C.F. 460

VI. Conclusion et décision

[194] La demande en l'espèce a donné à la Cour de prendre connaissance d'informations détaillées sur certains aspects du mandat relatif au renseignement étranger que confère au Service l'article 16 de la Loi sur le SCRS. En particulier, le Service a expliqué ses politiques et pratiques eu égard à la collecte, de manière incidente, d'informations sur des Canadiens, dont des élus, et à la conduite en parallèle d'opérations relevant des articles 12 et 16. Dans ces deux domaines, j'ai constaté que, dans l'ensemble, la conduite du Service est adéquate et satisfaisante. Je suggère cependant au Service de se donner des lignes directrices sur la diffusion d'informations pouvant permettre de reconnaître des Canadiens dont les communications ont été interceptées de manière incidente et sur le renversement de la divulgation minimale les concernant, et de donner à la Cour la possibilité de les commenter. Le Service devrait aussi informer la Cour des cas possibles d'interception, de manière incidente, de communications d'élus ou de fonctionnaires, ce qui permettrait à la Cour de fixer toute condition nécessaire à l'exécution des mandats. Il pourrait s'agir d'imposer au Service de lui redemander des directives sur le traitement des informations recueillies.

[195] En outre, je suis d'accord avec les modifications proposées par le Service aux modèles de mandats relatifs à l'article 16.

[196] Je conclus que l'article 16 constitue, pour le Service, une autorisation légale suffisante pour effectuer des fouilles minimalement envahissantes en vue de recueillir des renseignements étrangers. L'utilisation d'ESB telle que proposée par le Service entre dans cette catégorie de fouilles et, partant, ne nécessite pas de mandat.

[197] Toutefois, je constate que l'interception de données [***] dans la mesure où elle permet de découvrir [***] d'une personne, est plus que minimalement envahissante. [***] d'une personne permettrait au

inferences about his or her personal lifestyle choices [***] To comply with section 8 of the Charter, these searches require a judicially-authorized warrant.

[198] Finally, the Service’s interception on Canadian soil of communications of [***foreign persons***] who are outside Canada complies with the geographical limitation in section 16. These interceptions occur “within Canada.”

JUDGMENT in [***]

THIS COURT’S JUDGMENT is that:

1. The Service should develop guidelines for distributing and unminimizing the identities of Canadians whose communications have been incidentally intercepted under section 16, provide the Court an opportunity to comment on them, and specifically disclose to the Court when there is a possibility that the communications of an elected official or other public servant may be intercepted;
2. Section 16 provides sufficient legal authority for the use of CSS technology, in the manner proposed by the Service, without a warrant.
3. The interception of [***] data, to the extent that it captures a person’s [***], is more than minimally intrusive and requires a warrant.
4. The Service’s interception on Canadian soil of the communications of [***foreign persons***] who are outside Canada complies with the geographical limitation in section 16 as they occur “within Canada.”
5. Counsel for the Attorney General of Canada shall, within 15 days, make suggestions for information in this decision that should be redacted before it is released publicly. The *amicus* shall have 15 days

Service de tirer des conclusions quant à son mode de vie, [***] Pour respecter l’article 8 de la Charte, de telles fouilles requièrent l’obtention d’un mandat décerné par un tribunal.

[198] Enfin, l’interception par le Service, en sol canadien, de communications [***des personnes étrangères***] qui se trouvent à l’extérieur du Canada respecte la restriction géographique prévue à l’article 16 : de telles interceptions ont lieu « dans les limites du Canada ».

JUGEMENT DANS LE DOSSIER [***]

LA COUR STATUE que :

1. Le Service devrait se donner des lignes directrices sur la diffusion d’informations pouvant permettre de reconnaître des Canadiens dont les communications ont été interceptées de manière incidente et sur le renversement de la divulgation minimale les concernant, donner à la Cour la possibilité de les commenter et informer la Cour des cas possibles d’interception, de manière incidente, de communications d’élus ou de fonctionnaires.
2. L’article 16 constitue, pour le Service, une autorisation légale suffisante pour recourir aux ESB sans mandat, de la manière proposée.
3. L’interception de données [***] dans la mesure où elle permet de découvrir [***] d’une personne, est plus que minimalement envahissante et nécessite un mandat.
4. L’interception par le Service, en sol canadien, de communications [***des personnes étrangères***] qui se trouvent à l’extérieur du Canada respecte la restriction géographique prévue à l’article 16 : de telles interceptions ont lieu « dans les limites du Canada ».
5. Dans les 15 jours, l’avocat du procureur général présentera ses suggestions quant aux informations à caviarder dans la présente décision en vue de sa diffusion publique. L’*amicus* disposera ensuite de

from the receipt of those suggestions to make submissions on them. It is understood that counsel shall make every effort to keep redactions to a minimum.

15 jours pour présenter ses observations à leur sujet. Il est entendu que les avocats s'efforceront de caviarder le moins de passages possible.

ANNEX

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

INTERPRETATION

Definitions

2 In this Act,

...

threats to the security of Canada means

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

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

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

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

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

...

ANNEXE

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

DÉFINITIONS

Définitions

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

[...]

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

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

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

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

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

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

[...]

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.

Measures to reduce threats to the security of Canada

12.1 (1) If there are reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada, the Service may take measures, within or outside Canada, to reduce the threat.

Limits

(2) The measures shall be reasonable and proportional in the circumstances, having regard to the nature of the threat, the nature of the measures and the reasonable availability of other means to reduce the threat.

Warrant

(3) The Service shall not take measures to reduce a threat to the security of Canada if those measures will contravene a right or freedom guaranteed by the *Canadian Charter of Rights and Freedoms* or will be contrary to other Canadian law, unless the Service is authorized to take them by a warrant issued under section 21.1.

Clarification

(4) For greater certainty, nothing in subsection (1) confers on the Service any law enforcement power.

Prohibited conduct

12.2 (1) In taking measures to reduce a threat to the security of Canada, the Service shall not

(a) cause, intentionally or by criminal negligence, death or bodily harm to an individual;

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.

Mesures pour réduire les menaces envers la sécurité du Canada

12.1 (1) S'il existe des motifs raisonnables de croire qu'une activité donnée constitue une menace envers la sécurité du Canada, le Service peut prendre des mesures, même à l'extérieur du Canada, pour réduire la menace.

Limites

(2) Les mesures doivent être justes et adaptées aux circonstances, compte tenu de la nature de la menace et des mesures, ainsi que des solutions de rechange acceptables pour réduire la menace.

Mandat

(3) La prise par le Service de mesures pour réduire une menace envers la sécurité du Canada est subordonnée à l'obtention d'un mandat au titre de l'article 21.1 s'il s'agit de mesures qui porteront atteinte à un droit ou à une liberté garantis par la *Charte canadienne des droits et libertés* ou qui seront contraires à d'autres règles du droit canadien.

Précision

(4) Il est entendu que le paragraphe (1) ne confère au Service aucun pouvoir de contrôle d'application de la loi.

Interdictions

12.2 (1) Dans le cadre des mesures qu'il prend pour réduire une menace envers la sécurité du Canada, le Service ne peut :

a) causer, volontairement ou par négligence criminelle, des lésions corporelles à un individu ou la mort de celui-ci;

(b) wilfully attempt in any manner to obstruct, pervert or defeat the course of justice; or

(c) violate the sexual integrity of an individual.

Definition of *bodily harm*

(2) In subsection (1), ***bodily harm*** has the same meaning as in section 2 of the *Criminal Code*.

...

Collection of information concerning foreign states and persons

16 (1) Subject to this section, the Service may, in relation to the defence of Canada or the conduct of the international affairs of Canada, assist the Minister of National Defence or the Minister of Foreign Affairs, within Canada, in the collection of information or intelligence relating to the capabilities, intentions or activities of

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

(b) any person other than

(i) a Canadian citizen,

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

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

Limitation

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

Personal consent of Ministers required

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

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

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

b) tenter volontairement de quelque manière d'entraver, de détourner ou de contrecarrer le cours de la justice;

c) porter atteinte à l'intégrité sexuelle d'un individu.

Définition de *lésions corporelles*

(2) Au paragraphe (1), ***lésions corporelles*** s'entend au sens de l'article 2 du *Code criminel*.

[...]

Assistance

16 (1) Sous réserve des autres dispositions du présent article, le Service peut, dans les domaines de la défense et de la conduite des affaires internationales du Canada, prêter son assistance au ministre de la Défense nationale ou au ministre des Affaires étrangères, dans les limites du Canada, à la collecte d'informations ou de renseignements sur les moyens, les intentions ou les activités :

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

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

(i) les citoyens canadiens,

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

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

Restriction

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

Consentement personnel des ministres

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

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

b) au consentement personnel écrit du ministre.

...

[...]

PART II**JUDICIAL CONTROL****Application for warrant**

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

Matters to be specified in application for warrant

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

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

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

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

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

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

PARTIE II**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 confiées en vertu de l'article 16.

Contenu de la demande

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

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

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

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

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

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

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

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

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

Issuance of warrant

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

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

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

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

Activities outside Canada

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

Matters to be specified in warrant

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

(a) the type of communication authorized to be intercepted, the type of information, records, documents

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

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

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

Délivrance du mandat

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

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

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

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

Activités à l'extérieur du Canada

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

Contenu du mandat

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

a) les catégories de communications dont l'interception, les catégories d'informations, de documents ou

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

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

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

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

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

Maximum duration of warrant

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

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

(b) one year in any other case.

Application for warrant — measures to reduce threats to the security of Canada

21.1 (1) If the Director or any employee who is designated by the Minister for the purpose believes on reasonable grounds that a warrant under this section is required to enable the Service to take measures, within or outside Canada, to reduce a threat to the security of Canada, 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

(2) An application to a judge under subsection (1) shall be made in writing and be accompanied by the applicant's affidavit deposing to the following matters:

(a) the facts relied on to justify the belief on reasonable grounds that a warrant under this section is required to

d'objets dont l'acquisition, ou les pouvoirs visés aux alinéas (3)a) à c) dont l'exercice, sont autorisés;

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

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

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

e) la durée de validité du mandat;

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

Durée maximale

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

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

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

Demande de mandat — mesures pour réduire les menaces envers la sécurité du Canada

21.1 (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 prendre, au Canada ou à l'extérieur du Canada, des mesures pour réduire une menace envers la sécurité du Canada.

Contenu de la demande

(2) La demande 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

enable the Service to take measures to reduce a threat to the security of Canada;

(b) the measures proposed to be taken;

(c) the reasonableness and proportionality, in the circumstances, of the proposed measures, having regard to the nature of the threat, the nature of the measures and the reasonable availability of other means to reduce the threat;

(d) the identity of the persons, if known, who are directly affected by the proposed measures;

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

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

(g) the period, not exceeding 60 days or 120 days, as the case may be, for which the warrant is requested to be in force that is applicable by virtue of subsection (6); and

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

Issuance of warrant

(3) Despite any other law but subject to the *Statistics Act*, if the judge to whom an application under subsection (1) is made is satisfied of the matters referred to in paragraphs (2)(a) and (c) that are set out in the affidavit accompanying the application, the judge may issue a warrant authorizing the persons to whom it is directed to take the measures specified in it and, for that purpose,

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

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

est nécessaire pour permettre au Service de prendre des mesures pour réduire une menace envers la sécurité du Canada;

b) les mesures envisagées;

c) le fait que les mesures envisagées sont justes et adaptées aux circonstances, compte tenu de la nature de la menace et des mesures, ainsi que des solutions de rechange acceptables pour réduire la menace;

d) l'identité des personnes qui sont touchées directement par les mesures envisagées, si elle est connue;

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

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

g) la durée de validité applicable en vertu du paragraphe (6), de soixante jours ou de cent vingt jours au maximum, selon le cas, demandée pour le mandat;

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

Délivrance du mandat

(3) Par dérogation à toute autre règle de droit mais sous réserve de la *Loi sur la statistique*, le juge à qui est présentée la demande visée au paragraphe (1) peut décerner le mandat s'il est convaincu de l'existence des faits qui sont mentionnés aux alinéas (2)a) et c) et énoncés dans l'affidavit qui accompagne la demande; le mandat autorise ses destinataires à prendre les mesures qui y sont indiquées. À cette fin, il peut autoriser aussi, de leur part :

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

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

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

(d) to do any other thing that is reasonably necessary to take those measures.

Measures taken outside Canada

(4) Without regard to any other law, including that of any foreign state, a judge may, in a warrant issued under subsection (3), authorize the measures specified in it to be taken outside Canada.

Matters to be specified in warrant

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

(a) the measures authorized to be taken;

(b) the identity of the persons, if known, who are directly affected by the measures;

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

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

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

(f) any terms and conditions that the judge considers advisable in the public interest.

Maximum duration of warrant

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

(a) 60 days if the warrant is issued to enable the Service to take measures to reduce a threat to the security of Canada within the meaning of paragraph (d) of the definition *threats to the security of Canada* in section 2; or

(b) 120 days in any other case.

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

d) les autres actes nécessaires dans les circonstances à la prise des mesures.

Mesures à l'extérieur du Canada

(4) Sans égard à toute autre règle de droit, notamment le droit de tout État étranger, le juge peut autoriser la prise à l'extérieur du Canada des mesures indiquées dans le mandat décerné en vertu du paragraphe (3).

Contenu du mandat

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

a) les mesures autorisées;

b) l'identité des personnes qui sont touchées directement par les mesures, si elle est connue;

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

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

e) la durée de validité du mandat;

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

Durée maximale

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

a) de soixante jours, lorsque le mandat est décerné pour permettre au Service de prendre des mesures pour réduire une menace envers la sécurité du Canada au sens de l'alinéa d) de la définition de telles menaces à l'article 2;

b) de cent vingt jours, dans tout autre cas.