CSIS-28-18
2019 FC 141

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

And in the Matter of Islamist Terrorism – [***]

Indexed as: Sections 12 and 21 of the Canadian Security Intelligence Service Act, R.S.C., 1985, c. C-23 (Re)

Federal Court, Fothergill J.—Ottawa, September 25, 2018 and February 1, 2019.

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

Security Intelligence — Application for warrants pursuant to Canadian Security Intelligence Service Act, R.S.C., 1985, c. C-23, ss. 12, 21 in furtherance of ongoing investigation by Canadian Security Intelligence Service (CSIS) into Islamist terrorism, named individual — Warrants authorizing CSIS to install collection implant on computer, cellphone devices without user's knowledge — CSIS performing survey of device prior to intercepting communications — Survey information used to determine whether device owned, leased or used by subject of investigation — Survey information destroyed if device not meeting this condition — Survey information retained if CSIS believing device used by subject — Third party devices also subject to warrants — Whether proposed safeguards during survey stage sufficient to protect Canadian Charter of Rights and Freedom, privacy rights or interests of innocent third parties — Remotely installed implant may enable CSIS to intercept information from device used by innocent third party — Destruction of seized data not only way to limit invasiveness of search — Warrant itself may minimize intrusion into Charter rights, privacy interests of third parties — Minimization conditions in warrants required in some cases — Warrants having to fulfil objectives of prior authorization — Authorizing justices having discretion to impose conditions — Minimization conditions required in warrants authorizing remote installation of implants on devices — Warrants granted herein under search protocols sufficiently robust to safeguard Charter, privacy rights or interests of innocent parties — Application allowed.

CSIS-28-18
2019 CF 141

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

Et dans l'affaire visant le terrorisme islamiste – [***]

Répertorié : Articles 12 et 21 de la Loi sur le Service canadien du renseignement de sécurité, L.R.C. (1985), ch. C-23 (Re)

Cour fédérale, juge Fothergill—Ottawa, 25 septembre 2018 et 1er février 2019.

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

Renseignement de sécurité — Demande de mandats présentée en vertu des art. 12 et 21 de la Loi sur le Service canadien du renseignement de sécurité, L.R.C. (1985), ch. C-23, dans le cadre d'une enquête menée par le Service canadien du renseignement de sécurité (SCRS) sur le terrorisme islamiste et une personne connue — Les mandats autorisaient le SCRS à installer un implant destiné à la collecte dans un ordinateur ou un appareil de communication portable à l'insu de l'utilisateur — Avant que commence l'interception des communications, le SCRS effectue une analyse (survey) de l'appareil — Il détermine, au moyen des informations issues de l'analyse, si l'appareil est un appareil dont la cible est propriétaire ou qu'elle loue ou utilise — Si l'appareil ne satisfait pas à cette condition, les informations issues de l'analyse doivent être détruites — Le SCRS conserve les informations obtenues lors de l'analyse s'il croit que la cible utilise l'appareil — L'appareil appartenant à un tiers a aussi été visé par les mandats — Il s'agissait de savoir si les mesures proposées à l'étape de l'analyse suffisaient à protéger les droits garantis par la Charte canadienne des droits et libertés et le droit au respect de la vie privée des tiers innocents — Grâce à un implant installé à distance, le Service peut intercepter des informations sur un appareil qu'un tiers innocent utilise — La destruction des données obtenues n'est qu'une des manières de limiter le caractère intrusif de la fouille — Le mandat lui-même peut minimiser l'empiètement sur les droits garantis par la Charte et sur le droit des tiers au respect de leur vie privée — Des conditions prévoyant la réduction au minimum des répercussions peuvent être nécessaires dans un mandat dans certains cas — Les mandats doivent répondre aux objectifs de la procédure d'autorisation préalable — Le juge saisi de la demande

Constitutional Law — Charter of Rights — Unreasonable Search or Seizure — Warrants sought pursuant to Canadian Security Intelligence Service Act, R.S.C., 1985, c. C-23, ss. 12, 21 in furtherance of ongoing investigation by Canadian Security Intelligence Service (CSIS) into Islamist terrorism, named individual — Warrants authorizing CSIS to install collection implant on computer, cellphone devices without user's knowledge — Raising questions regarding compliance with Charter, privacy rights or interests of affected persons — CSIS performing survey of device prior to intercepting communications — Survey information used to determine whether device owned, leased or used by subject of investigation — Survey information destroyed if device not meeting this condition — Survey information retained if CSIS believing device used by subject — Third party devices subject to warrants — Whether proposed safeguards during survey stage sufficient to protect Canadian Charter of Rights and Freedom, privacy rights or interests of innocent third parties — Destruction of seized data not only way to limit invasiveness of search — Warrant itself may minimize intrusion into Charter rights, privacy interests of third parties — Minimization conditions required in warrants authorizing remote installation of implants on devices — Warrants granted herein under search protocols sufficiently robust to safeguard Charter, privacy rights or interests of innocent parties.

This was an application for warrants pursuant to sections 12 and 21 of the *Canadian Security Intelligence Service Act*, R.S.C., 1985, c. C-23 in furtherance of an ongoing investigation by the Canadian Security Intelligence Service (CSIS) into Islamist terrorism and a named individual.

Two of those warrants authorized CSIS to install a collection implant on a device such as a computer or cellphone in order to intercept communications and obtain information. Collection

Droit constitutionnel — Charte des droits — Fouilles, perquisitions ou saisies abusives — Demande de mandats présentée en vertu des art. 12 et 21 de la Loi sur le Service canadien du renseignement de sécurité, L.R.C. (1985), ch. C-23, dans le cadre d'une enquête menée par le Service canadien du renseignement de sécurité (SCRS) sur le terrorisme islamiste et une personne connue — Les mandats autorisaient le SCRS à installer un implant destiné à la collecte dans un ordinateur ou un appareil de communication portable à l'insu de l'utilisateur — Ils ont soulevé des questions relatives aux droits garantis par la Charte et au droit au respect de la vie privée des personnes qui pourraient être touchées — Le SCRS effectue une analyse (survey) de l'appareil avant que commence l'interception des communications — Il détermine, au moyen des informations issues de l'analyse, si l'appareil est un appareil dont la cible est propriétaire ou qu'elle loue ou utilise — Si l'appareil ne satisfait pas à cette condition, les informations issues de l'analyse doivent être détruites — Le SCRS conserve les informations obtenues lors de l'analyse s'il croit que la cible utilise l'appareil — L'appareil appartenant à un tiers était aussi visé par les mandats — Il s'agissait de savoir si les mesures proposées à l'étape de l'analyse suffisent à protéger les droits garantis par la Charte canadienne des droits et libertés et le droit au respect de la vie privée des tiers innocents — La destruction des données obtenues n'est qu'une des manières de limiter le caractère intrusif de la fouille — Le mandat lui-même peut minimiser l'empiètement sur les droits garantis par la Charte et sur le droit des tiers au respect de leur vie privée — Des conditions prévoyant la réduction au minimum des répercussions peuvent être nécessaires dans un mandat dans certains cas — Les mandats ont été décernés dans la présente affaire sur le fondement de protocoles de fouille suffisamment rigoureux pour protéger les droits garantis par la Charte et le droit des tiers innocents.

Il s'agissait d'une demande de mandats présentée en vertu des articles 12 et 21 de la *Loi sur le Service canadien du renseignement de sécurité*, L.R.C. (1985), ch. C-23, dans le cadre d'une enquête menée par le Service canadien du renseignement de sécurité (SCRS) sur le terrorisme islamiste et une personne connue.

Deux de ces mandats autorisaient le SCRS à installer un implant destiné à la collecte dans un ordinateur ou un appareil de communication portable en vue d'intercepter des

from an implant is done on an ongoing basis without the user's knowledge. Certain powers sought in the warrants were novel, and could raise questions regarding compliance with the *Canadian Charter of Rights and Freedom* (Charter), and the privacy rights or interests of persons who could be affected by their exercise. The new powers sought in the warrants were intended to reflect the practical reality that CSIS may not be able to determine, prior to installing an implant, whether the device belongs to or is used by the subject of investigation. Where an implant is remotely installed, a survey of the device is performed prior to intercepting communications. A CSIS employee reviews the survey information and determines whether the device is (a) a portable device owned, leased or used by the subject of investigation; or (b) a computer holding information that may be obtained pursuant to the general intercept and search warrant. If the device does not fall within one of these two categories, then the survey information is destroyed as soon as reasonably practicable, but no later than six months from the date it was obtained. If the device is neither owned nor leased by the subject of investigation, but the CSIS employee has reasonable grounds to believe that it is used by the subject, then the Regional Director General may authorize interception. Survey information which may assist the Regional Director General's exercise of this responsibility may be retained for this purpose. Devices belonging to third parties would also be subjected to the warrants. CSIS would be able to distinguish a third party device from the device belonging to or used by the subject of investigation. If information regarding a third party device does not relate to a subject of investigation, it is destroyed as soon as reasonably practicable.

The issue raised by these warrant applications was whether the safeguards proposed by CSIS during the survey stage were sufficient to protect the Charter and privacy rights or interests of innocent third parties whose personal information may be collected during the remote installation of an implant on a device.

Held, the application should be allowed.

A remotely installed implant may enable CSIS to intercept information from a device that is used by or belongs to an innocent third party. Canadian case law addressing the legal implications of remotely installed implants is sparse. The destruction of data seized from innocent third parties is one way to limit the invasiveness of an electronic search, but it is not the only one. The warrant itself may minimize intrusion into the Charter rights and privacy interests of third parties. In *R. v. Thompson*, the Supreme Court considered a "'resort to'" clause that would authorize the police to monitor communications

communications et d'obtenir des informations. Il s'agit d'une collecte qui s'effectue en continu, à l'insu de l'utilisateur. Les mandats demandés prévoyaient certains pouvoirs nouveaux qui pourraient soulever des questions relatives aux droits garantis par la *Charte canadienne des droits et libertés* (Charte) et au droit au respect de la vie privée des personnes que l'exercice de ces pouvoirs pourrait toucher. Les nouveaux pouvoirs demandés dans les mandats étaient censés prévoir qu'en pratique, le SCRS peut ne pas être en mesure de déterminer, avant l'installation, que l'appareil appartient à la cible ou est utilisé par elle. Avant que commence l'interception des communications dans un appareil où un implant a été installé à distance, une analyse (*survey*) de l'appareil est effectuée. Un employé du SCRS détermine, au moyen des informations issues de l'analyse, si l'appareil est a) un appareil portable dont la cible est propriétaire ou qu'elle loue ou utilise, ou b) un ordinateur qui contient des informations pouvant être obtenues en vertu du mandat sur les interceptions générales et les fouilles. Si l'appareil n'entre pas dans l'une ou l'autre de ces deux catégories, les informations issues de l'analyse sont détruites dès qu'il est matériellement possible de le faire, dans les six mois suivant l'obtention. Le directeur général régional peut autoriser l'interception des communications effectuées au moyen d'un appareil dont la cible de l'enquête n'est pas propriétaire et qu'elle n'a pas loué, si l'employé du SCRS a des motifs raisonnables de croire que celle-ci l'utilise. Il est possible de conserver les informations obtenues lors de l'analyse qui peuvent aider le directeur général régional à s'acquitter de cette responsabilité, à cette fin. L'appareil appartenant à un tiers était aussi visé par les mandats. Le SCRS serait en mesure de distinguer cet appareil de l'appareil dont la cible était propriétaire ou qu'elle utilisait. Il devait détruire cette information si elle n'était pas liée à une cible d'enquête dès qu'il lui serait matériellement possible de le faire.

La demande de mandats a soulevé la question de savoir si les mesures proposées par le Service à l'étape de l'analyse suffisaient à protéger les droits garantis par la Charte et le droit au respect de la vie privée des tiers innocents dont il pourrait recueillir les renseignements personnels dans le cadre de l'installation à distance d'un implant dans un appareil.

Jugement : la demande doit être accueillie.

Grâce à un implant installé à distance, le Service peut intercepter des informations sur un appareil dont un tiers innocent est propriétaire ou qu'il utilise. Au Canada, les précédents ayant trait aux conséquences juridiques de l'installation d'implants à distance sont peu nombreux. La destruction des données obtenues auprès de tiers innocents n'est qu'une des manières de limiter le caractère intrusif de la fouille. Le mandat lui-même peut minimiser l'empiètement sur les droits garantis par la Charte et sur le droit des tiers au respect de leur vie privée. Dans l'arrêt *R. c. Thompson*, la Cour suprême du Canada a

from a location the target may "'resort to'". The "resort to" clause was not found to be unlawful in *Thomson*; however, a total absence of any protection for the public created a potential for carrying out unreasonable searches and seizures. The principle remained valid and applicable here. Minimization conditions in a warrant may be required in some cases depending on the extent of the potential invasion of the privacy of innocent third parties. While search protocols may not be constitutionally required in all cases, authorizing justices must assure themselves that the warrants they issue fulfil the objectives of prior authorization. They also have the discretion to impose conditions to ensure they do. Given the extent of the potential invasion of the privacy of innocent third parties, the parties agreed herein that minimization conditions were required in warrants that authorize the remote installation of implants on devices. The survey stage was made mandatory before full data collection could commence and the data collected at that stage was limited to specific categories. With these modifications, the searches to be conducted under the warrants requested were reasonable. The search protocols were sufficiently robust to safeguard the Charter and privacy rights or interests of innocent parties. The warrants were therefore granted, but could only be issued with the search protocols set out herein.

étudié une disposition sur les « "endroits fréquentés" » qui autoriserait la police à surveiller les communications effectuées à un endroit que la cible est susceptible de fréquenter. Dans l'arrêt *Thompson*, la disposition sur les « endroits fréquentés » n'a pas été jugée contrevenir à la loi; toutefois, l'absence totale de toute mesure de protection du public entraînait la possibilité que soient effectuées des fouilles, des perquisitions ou des saisies abusives. Ce principe est demeuré valable et s'appliquait en l'espèce. Il se peut que des conditions prévoyant la réduction au minimum des répercussions dans un mandat soient nécessaires dans certains cas, selon l'ampleur de l'atteinte possible à la vie privée de tiers innocents. S'il est possible que des protocoles de fouille ne soient pas constitutionnellement requis en toutes circonstances, le juge saisi de la demande d'autorisation doit s'assurer que les mandats qu'il décerne répondent aux objectifs de la procédure d'autorisation préalable. Il possède en outre le pouvoir discrétionnaire d'imposer des conditions à cette fin. Compte tenu de l'ampleur de l'atteinte éventuelle à la vie privée de tiers innocents, les parties ont convenu dans la présente affaire que les mandats qui autorisent l'installation à distance d'implants dans des appareils doivent comporter des mesures de réduction au minimum des répercussions. L'étape de l'analyse a été rendue obligatoire avant que la collecte de données puisse commencer, et les données obtenues à l'étape de l'analyse se sont limitées à certaines catégories. Moyennant l'apport de ces modifications, les fouilles à effectuer en vertu des mandats demandés étaient raisonnables. Les protocoles de fouille étaient suffisamment rigoureux pour protéger les droits garantis par la Charte et le droit des tiers innocents. Partant, les mandats ont été décernés, mais pour être décernés, ils devaient comporter les protocoles de fouille qui ont été énoncés en l'espèce.

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. 12, 21.
Criminal Code, R.S.C., 1985, c. C-46.

LOIS ET RÈGLEMENTS CITÉS

Charte canadienne des droits et libertés, qui constitue la partie I de la *Loi constitutionnelle de 1982*, annexe B, *Loi de 1982 sur le Canada*, 1982, ch. 11 (R.-U.) [L.R.C. (1985), appendice II, nº 44], art. 8.
Code criminel, L.R.C. (1985), ch. C-46.
Loi sur le Service canadien du renseignement de sécurité, L.R.C. (1985), ch. C-23, art. 12, 21.

CASES CITED

APPLIED:

R. v. Thompson, [1990] 2 S.C.R. 1111, (1990), 73 D.L.R. (4th) 596.

CONSIDERED:

Atwal v. Canada, [1988] 1 F.C. 107 (1987), 28 Admin. L.R. 92 (C.A.); *R. v. Vu*, 2013 SCC 60, [2013] 3 S.C.R. 657; *R. v. Marakah*, 2017 SCC 59, [2017] 2 S.C.R. 608; *In re Warrant*

JURISPRUDENCE CITÉE

DÉCISION APPLIQUÉE :

R. c. Thompson, [1990] 2 R.C.S. 1111.

DÉCISIONS EXAMINÉES :

Atwal c. Canada, [1988] 1 C.F. 107 (C.A.); *R. c. Vu*, 2013 CSC 60, [2013] 3 R.C.S. 657; *R. c. Marakah*, 2017 CSC 59, [2017] 2 R.C.S. 608; *In re Warrant to Search a Target*

to Search a Target Computer at Premises Unknown, 2013 WL 1729765, 958 F. Supp. 2d 753 (U.S. Dist. Ct.).

REFERRED TO:

Canada (Attorney General) v. Huang, 2018 FCA 109, 362 C.C.C. (3d) 87.

AUTHORS CITED

Chand, Gerald, *Digital Evidence: A Practitioner's Handbook*. Toronto: Emond Montgomery Publications Limited, 2018.

Jones, Brock. "Modern Technology and Privacy Rights: Leading Canadian and U.S. Case Law" Ontario Bar Association Criminal Justice, Vol. 22, No. 10, June 2013.

Owsley, Brian L. "Beware of Government Agents Bearing Trojan Horses" (2015), 48 *Akron L. Rev.* 314.

APPLICATION for warrants pursuant to sections 12 and 21 of the *Canadian Security Intelligence Service Act*, R.S.C., 1985, c. C-23 in furtherance of an ongoing investigation by the Canadian Security Intelligence Service into Islamist terrorism and a named individual. Application allowed.

APPEARANCES

Stéphanie Dion and *Andrew Cameron* for applicant.
Ian Carter as *amicus curiae*.

SOLICITORS OF RECORD

Deputy Attorney General of Canada for applicant.

Bayne Sellar Ertel Carter, Ottawa, as *amicus curiae*.

The following are the reasons for order rendered in English by

FOTHERGILL J.:

I. Overview

[1] On October 16, 2018, I issued a series of warrants pursuant to sections 12 and 21 of the *Canadian Security*

Computer at Premises Unknown, 2013 WL 1729765, 958 F. Supp. 2d 753 (U.S. Dist. Ct.).

DÉCISION CITÉE :

Canada (Procureur général) c. Huang, 2018 CAF 109.

DOCTRINE CITÉE

Chand, Gerald, *Digital Evidence : A Practitioner's Handbook*. Toronto : Emond Montgomery Publications Limited, 2018.

Jones, Brock. « Modern Technology and Privacy Rights : Leading Canadian and U.S. Case Law » L'Association du Barreau de l'Ontario Justice pénale, vol. 22, nº 10, juin 2013.

Owsley, Brian L. « Beware of Government Agents Bearing Trojan Horses » (2015), 48 *Akron L. Rev.* 314.

DEMANDE de mandats présentée en vertu des articles 12 et 21 de la *Loi sur le Service canadien du renseignement de sécurité*, L.R.C. (1985), ch. C-23, dans le cadre d'une enquête menée par le Service canadien du renseignement de sécurité sur le terrorisme islamiste et une personne connue. Demande accueillie.

ONT COMPARU :

Stéphanie Dion et *Andrew Cameron*, pour le demandeur.
Ian Carter, à titre d'*amicus curiae*.

AVOCATS INSCRITS AU DOSSIER

La sous-procureure générale du Canada, pour le demandeur.
Bayne Sellar Ertel Carter, Ottawa, à titre d'*amicus curiae*.

Voici les motifs de l'ordonnance rendus en français par

LE JUGE FOTHERGILL :

I. Aperçu

[1] Le 16 octobre 2018, j'ai décerné une série de mandats en vertu des articles 12 et 21 de la *Loi sur le Service*

Intelligence Service Act, R.S.C., 1985, c. C-23 (CSIS Act) in furtherance of an ongoing investigation by the Canadian Security Intelligence Service (CSIS or the Service) into Islamist terrorism and a named individual. Two of those warrants authorize the Director of CSIS and any employee of the Service acting under his authority to install, maintain, remove [***] "any thing" on a computer or portable communications device in order to intercept communications and obtain information. This technique is commonly described as installing an "implant" on a device.

[2] In effect, a collection implant enables the Service to covertly receive a copy of what a subject of investigation [***] on a computer or portable communications device (collectively, device). The Service also uses implants to conduct remote searches of devices and obtain information including, but not limited to, images, documents, e-mail messages, [***]. Collection from an implant is done on an ongoing basis without the user's knowledge.

[3] Counsel representing the Attorney General of Canada acknowledged that certain powers sought in the warrants are novel, and could raise questions regarding compliance with the *Canadian Charter of Rights and Freedoms*[1] (Charter), and the privacy rights or interests of persons who could be affected by their exercise. The Court convened an oral hearing to hear from counsel for the Attorney General, the CSIS employee who applied for the warrants, and two additional affiants.

[4] The Court also appointed a security-cleared *amicus curiae*. The *amicus curiae* was given access to relevant documents, and was offered the opportunity to cross-examine all affiants and make submissions orally and in writing. The Court directed the *amicus curiae* to present his considered and professional opinion regarding the legal and other issues raised by the application. The *amicus curiae* was not obliged to adopt an adversarial position if he did not consider this to be necessary or justified.

[1] being art 1 of the *Constitution Act, 1982*, Schedule B, *Canada Act 1982*, 1982, c. 11 (U.K.) [R.S.C. 1985, Appendix II, No. 44].

canadien du renseignement de sécurité, L.R.C. (1985), ch. C-23 (Loi sur le SCRS) dans le cadre d'une enquête menée par le Service canadien du renseignement de sécurité (SCRS ou Service) sur le terrorisme islamiste et une personne connue. Deux de ces mandats autorisent le directeur du SCRS et tout employé agissant sous son autorité à installer tout « objet » dans un ordinateur ou un appareil de communication portable, à l'entretenir, à l'enlever [***], en vue d'intercepter des communications et d'obtenir des informations. Il s'agit de la technique qui, généralement parlant, consiste à installer un « implant » dans un appareil.

[2] En pratique, un implant destiné à la collecte permet au Service d'obtenir, en secret, une copie de ce que la cible [***] sur un ordinateur ou un appareil de communication portable (appareil) ou par l'entremise de celui-ci. Le Service a aussi recours à des implants pour fouiller des appareils à distance et obtenir des informations, notamment des images, des documents, des courriels, [***]. Il s'agit d'une collecte qui s'effectue en continu, à l'insu de l'utilisateur.

[3] L'avocat représentant la procureure générale du Canada a reconnu que les mandats demandés prévoient des pouvoirs nouveaux qui pourraient soulever des questions relatives aux droits garantis par la *Charte canadienne des droits et libertés*[1] (Charte) et au droit au respect de la vie privée des personnes que l'exercice de ces pouvoirs pourrait toucher. La Cour a entendu les observations orales de l'avocat de la procureure générale, de l'employé du SCRS qui a présenté la demande de mandats et de deux déposants.

[4] La Cour a aussi nommé un *amicus curiae* possédant l'habilitation de sécurité nécessaire. Celui-ci a eu accès aux documents utiles et a eu la possibilité de contre-interroger les déposants et de présenter des observations orales et écrites. La Cour a demandé à l'*amicus curiae* de lui faire part de son opinion réfléchie et professionnelle quant aux questions de nature juridique, entre autres, que soulevait la demande. L'*amicus curiae* n'était pas tenu d'adopter une position antagoniste s'il n'estimait pas que c'était nécessaire ou justifié.

[1] qui constitue la partie I de la *Loi constitutionnelle de 1982*, annexe B, *Loi de 1982 sur le Canada*, 1982, ch. 11 (R.-U.) [L.R.C. (1985), appendice II, nº 44].

[5] After hearing from the affiants, reading the materials filed, and considering the submissions of counsel for the Attorney General of Canada and the *amicus curiae*, I concluded that the requirements of paragraphs 21(2)(a) and (b) of the CSIS Act were met and the warrants should be issued with minor modifications. These are the reasons for that decision.

II. New Powers Sought

[6] Before installing an implant on a device, the Service seeks to identify the device used by the subject of its investigation. This is typically accomplished by recourse to human sources, surveillance, interviews, cell-site simulators, or requests to domestic or foreign law enforcement and intelligence agencies. It may also be facilitated by the interception of communications and information obtained from communications service providers. If the subject of investigation [***] CSIS may seek the assistance of the Communications Security Establishment to conduct the investigative steps authorized by the warrants.

[7] When performing a remote installation of an implant, the Service first collects preliminary information in order to confirm that the implant is being installed on a device that belongs to or is used by the subject of investigation. The new powers sought in the warrants are intended to reflect the practical reality that the Service may not be able to determine, prior to installing an implant, whether the device belongs to or is used by the subject of investigation.

[8] The warrants authorize employees of the Service to remotely install an implant on any device that is [***] by the subject of investigation; [***] by the subject of investigation. [***]

[9] Depending on the kind of implant used, the Service may require an Internet warrant to be in force. The Internet warrant authorizes the Service to intercept communications destined to or originating from an Internet services account [***] a subject of investigation.

[5] Après avoir entendu les déposants et pris connaissance des documents présentés ainsi que des observations de l'avocat de la procureure générale et de l'*amicus curiae*, j'ai conclu que la demande satisfaisait aux exigences prévues aux alinéas 21(2)a) et b) de la Loi sur le SCRS et que les mandats pouvaient être décernés sous réserve de modifications mineures. Voici les motifs de cette décision.

II. Nouveaux pouvoirs demandés

[6] Avant de procéder à l'installation d'un implant, le SCRS cherche à repérer l'appareil utilisé par la cible de l'enquête. Pour ce faire, il utilise habituellement les méthodes suivantes : recours à des sources humaines, filature, entrevues, utilisation d'émulateurs de station de base ou demande d'assistance à des services d'application de la loi ou de renseignement canadiens ou étrangers. Cette démarche peut aussi être facilitée par l'interception de communications et l'obtention d'informations auprès de fournisseurs de services de communication. Si la cible [***] le SCRS peut demander au Centre de la sécurité des télécommunications de lui prêter assistance dans les activités d'enquête menées en vertu des mandats.

[7] Lorsqu'il installe un implant à distance, le Service recueille au préalable des informations lui permettant de confirmer que l'implant sera bien installé dans un appareil dont la cible est propriétaire ou qu'elle utilise. Les nouveaux pouvoirs demandés dans les mandats sont censés prévoir qu'en pratique, le Service peut ne pas être en mesure de déterminer, avant l'installation, que l'appareil appartient à la cible ou est utilisé par elle.

[8] Les mandats autorisent les employés du SCRS à installer à distance un implant dans tout appareil [***] de la cible [***] de la cible. [***]

[9] Tout dépendant du type d'implant, le SCRS peut devoir obtenir un mandat sur Internet. Ce mandat l'autorise à intercepter les communications qui parviennent à un compte auprès d'un fournisseur de services Internet [***] de la cible [***] ou qui en proviennent.

[10] Where an implant is remotely installed on a device [***] a survey of the device is performed prior to intercepting communications and obtaining the information described in the warrants. The survey information may include: [***] operating system information, device make and model, network addresses, [***].

[11] Other information may also be obtained at the survey stage in order to protect the security of the implant: [***].

[12] Depending on whether the Service is operating pursuant to a portable device warrant or a general intercept and search warrant, a designated Service employee reviews the survey information and determines whether the device is (a) a portable device owned, leased or used by the subject of investigation; or (b) a computer holding information that may be obtained pursuant to the general intercept and search warrant. If the device falls within one of these two categories, then the survey information is retained and the interception and collection from the device commences. If the device does not fall within one of these two categories, then the survey information is destroyed as soon as reasonably practicable, but no later than six months from the date it was obtained.

[13] If the device is neither owned nor leased by the subject of investigation, but the designated Service employee has reasonable grounds to believe that it is used by the subject, then the Regional Director General may authorize interception. Survey information which may assist the Regional Director General's exercise of this responsibility may be retained for this purpose. Due to the exigencies of the investigation, the determination is usually made quickly.

[14] The warrants also authorize [***] using what is referred to as a [***]. A survey is not required for [***] because a determination has already been made that the implant has been installed on a device belonging to or used by a subject of investigation.

[10] Avant que commence l'interception des communications et l'obtention des informations mentionnées dans les mandats dans un appareil où un implant a été installé à distance [***] une analyse (*survey*) de l'appareil est effectuée, laquelle permet d'obtenir, en tout ou en partie, les informations suivantes : [***] informations sur le système d'exploitation, marque et modèle de l'appareil, adresses réseau, [***].

[11] D'autres informations peuvent être obtenues à cette étape afin d'assurer la sécurité de l'implant : [***].

[12] Selon que s'applique le mandat sur les appareils portables ou le mandat sur les interceptions générales et les fouilles, un employé du Service désigné détermine, au moyen des informations issues de l'analyse, si l'appareil est a) un appareil portable dont la cible est propriétaire ou qu'elle loue ou utilise ou b) un ordinateur qui contient des informations pouvant être obtenues en vertu du mandat sur les interceptions générales et les fouilles. Si l'appareil entre dans l'une ou l'autre de ces catégories, les informations issues de l'analyse sont conservées, et l'interception et la collecte commencent. Si ce n'est pas le cas, les informations en question sont détruites dès qu'il est matériellement possible de le faire, dans les six mois suivant l'obtention.

[13] Le directeur général régional peut autoriser l'interception des communications effectuées au moyen d'un appareil dont la cible de l'enquête n'est pas propriétaire et qu'elle n'a pas loué, si l'employé du Service désigné a des motifs raisonnables de croire que celle-ci l'utilise. Il est possible de conserver les informations obtenues lors de l'analyse qui peuvent aider le directeur général régional à s'acquitter de cette responsabilité, à cette fin. En général, les circonstances de l'enquête l'amènent à prendre la décision rapidement.

[14] Les mandats autorisent aussi [***] servant de [***] ne requiert pas d'analyse, car il a déjà été déterminé que l'implant a été installé dans un appareil dont la cible de l'enquête est propriétaire ou qu'elle utilise.

[15] In addition, the warrants authorize the [***] of a device belonging to a third party where the Service installs an implant on a device which is subsequently determined at the survey stage to be unconnected to the target of investigation. The warrants permit the Service to [***] the third party's device that will enable CSIS to distinguish it from the device belonging to or used by the subject of investigation. Once installed, the [***]. As this information does not relate to a subject of investigation, it is destroyed as soon as reasonably practicable, but no later than six months from the date it was obtained.

[16] While much of the information obtained at the survey stage will reveal little or no core biographical information about the individual who owns or uses the device, some of it may. Depending on [***] may disclose sensitive personal information. [***].

III. Issue

[17] The legal issue raised by these warrant applications is whether the safeguards proposed by the Service during the survey stage are sufficient to protect the Charter and privacy rights or interests of innocent third parties whose personal information may be collected during the remote installation of an implant on a device.

IV. Analysis

[18] The installation of an implant on a device is authorized under standard provisions of warrants that permit the interception of communications, the acquisition of information and images, and the tracking or geolocation of a subject of investigation. The Service has previously sought to intercept communications or obtain information from a device by remotely installing an implant. This technique, including the use of a survey stage to identify the correct device, was explained to the Court during an *en banc* presentation on December 15, 2017.

[19] In the course of the *en banc* presentation, Chief Justice Paul Crampton expressed the view that a survey

[15] En outre, les mandats autorisent [***] d'un appareil appartenant à un tiers, c'est-à-dire l'installation d'un implant dans un appareil qui, à l'issue de l'étape de l'analyse, s'avère ne pas avoir de lien avec la cible. Les mandats permettent au Service [***] dans l'appareil du tiers, [***] qui lui permettra de distinguer cet appareil de l'appareil dont la cible est propriétaire ou qu'elle utilise. [***]. Le SCRS détruit cette information, qui n'est pas liée à une cible d'enquête, dès qu'il lui est matériellement possible de le faire, dans les six mois suivant l'obtention.

[16] La plupart des informations obtenues à l'étape de l'analyse ne révéleront que peu d'informations biographiques de base sur la personne qui est propriétaire de l'appareil ou qui l'utilise, voire aucune; cependant, ce pourrait être le cas de certaines d'entre elles. Tout dépendant [***] peuvent révéler des renseignements personnels sensibles. [***].

III. Question

[17] La demande de mandats en l'espèce soulève le point de droit suivant : les mesures proposées par le Service à l'étape de l'analyse suffisent-elles à protéger les droits garantis par la Charte et le droit au respect de la vie privée des tiers innocents dont il pourrait recueillir les renseignements personnels dans le cadre de l'installation à distance d'un implant dans un appareil?

IV. Analyse

[18] Selon les dispositions habituelles des mandats autorisant l'interception de communications, l'acquisition d'informations et d'images ainsi que le repérage ou la géolocalisation d'une cible, le Service peut installer un implant dans un appareil. Le SCRS a déjà cherché à intercepter des communications ou à obtenir des informations provenant d'un appareil en y installant un implant à distance. Le 15 décembre 2017, une formation collégiale des juges de la Cour a reçu des explications relatives à cette technique et à l'étape de l'analyse consistant à repérer le bon appareil.

[19] Au cours de cet exposé, le juge en chef Paul Crampton s'est dit d'avis que l'étape de l'analyse devrait

stage should be mandatory before full data collection using an implant can begin. This is the first time the Court has been asked to consider the language of the new warrant condition.

A. *General Principles*

[20] The Court may grant a warrant enabling CSIS to collect information and intelligence under section 12 of the CSIS Act only when the requirements of subsection 21(2) are met. The Court must be satisfied, *inter alia*, that a warrant is required to investigate a threat to the security of Canada, and that other investigative measures have been tried and have either failed or are unlikely to succeed. The Federal Court of Appeal observed in *Atwal v. Canada*, [1988] 1 F.C. 107, at page 127 that "it will be generally less practically possible to be specific, in advance, in authorizations to intercept private communications under the [CSIS] Act than under the *Criminal Code*".

[21] A search pursuant to a CSIS warrant may be unreasonable and contrary to section 8 of the Charter if it is not carried out in a reasonable manner. This may be because the issuing justice failed to limit the breadth of the authorization, or because the persons carrying out the search failed to adhere to minimization principles in executing the warrants (*Canada (Attorney General) v. Huang*, 2018 FCA 109, 362 C.C.C. (3d) 87, at paragraph 28).

[22] There is a high expectation of privacy in a computer or a cell phone. As the Supreme Court of Canada held in *R. v. Vu*, 2013 SCC 60, [2013] 3 S.C.R. 657 [*Vu*], at paragraphs 40 to 44, it is difficult to imagine a more intrusive invasion of privacy than a search of these devices. Personal computers store immense amounts of information, some of which may touch the "'biographical core of personal information'". In addition, computers contain information that is automatically generated, often without the knowledge of the user, and a computer may retain files and data long after users think they have been deleted. When connected to the Internet, computers serve as portals to an almost infinite amount of

être obligatoire avant que la collecte de données au moyen d'un implant puisse commencer. La Cour se penchait alors pour la première fois sur le libellé de la nouvelle condition figurant dans les mandats.

A. *Principes généraux*

[20] La Cour ne peut décerner un mandat permettant au Service de recueillir des informations et des renseignements en vertu de l'article 12 de la Loi sur le SCRS que si les exigences prévues au paragraphe 21(2) de cette même loi sont respectées. Notamment, la Cour doit être convaincue que le mandat est nécessaire pour permettre au Service de faire enquête sur des menaces envers la sécurité du Canada et que d'autres méthodes d'enquête ont été essayées en vain ou semblent avoir peu de chances de succès. Dans l'arrêt *Atwal c. Canada*, [1988] 1 C.F. 107, à la page 127, la Cour d'appel fédérale a souligné que « les autorisations d'interception de communications privées fondées sur la [Loi sur le SCRS] seront, en pratique, plus difficilement précises à l'avance que les autorisations prévues au *Code criminel* ».

[21] Si elle n'est pas menée de manière raisonnable, une fouille effectuée en vertu d'un mandat décerné au SCRS peut être abusive, donc contraire à l'article 8 de la Charte. Il se peut que le juge qui a décerné le mandat ait omis de limiter la portée de l'autorisation ou que les personnes qui ont effectué la fouille n'aient pas souscrit aux principes de réduction au minimum des répercussions lorsqu'elles ont exécuté les mandats (*Canada (Procureur générale) c. Huang*, 2018 CAF 109, au paragraphe 28).

[22] S'agissant d'un ordinateur ou d'un téléphone, l'attente en matière de vie privée est élevée. Comme l'a soutenu la Cour suprême du Canada dans l'arrêt *R. c. Vu*, 2013 CSC 60, [2013] 3 R.C.S. 657 (*Vu*), aux paragraphes 40 à 44, il est difficile d'imaginer une atteinte plus grave à la vie privée que la fouille d'un de ces appareils. En effet, un ordinateur personnel contient d'immenses quantités d'informations, dont certaines touchent à l'« "ensemble de renseignements biographiques d'ordre personnel" ». En outre, les ordinateurs renferment des informations générées automatiquement, souvent à l'insu de l'utilisateur, et peuvent conserver des fichiers et des données longtemps après que l'utilisateur

information that is shared between different users and is stored almost anywhere in the world. Similarly, a computer that is connected to a network may allow police and intelligence agencies to obtain access to information on other devices.

[23] In *R. v. Marakah*, 2017 SCC 59, [2017] 2 S.C.R. 608, at paragraph 37, the Supreme Court of Canada remarked that electronic conversations are capable of revealing a great deal of personal information. Preservation of a "'zone of privacy'" in which personal information is safe from state intrusion is the very purpose of section 8 of the Charter. This zone of privacy extends beyond one's own mobile device. It can include electronic conversations in which one shares private information with others. It is reasonable to expect these private interactions, and not just the contents of a particular cell phone at a particular point in time, to remain private.

B. *Remote Searches*

[24] A remotely installed implant may enable CSIS to intercept [***] the installation of an implant on a device that is used by or belongs to an innocent third party is a real possibility. If the [***] is associated with a public place, such as an Internet café, it becomes highly likely.

[25] The *amicus curiae* informed the Court that Canadian jurisprudence addressing the legal implications of remotely installed implants is sparse. He referred the Court to the following excerpt from Gerald Chand and Susan Magotiaux, *Digital Evidence: A Practitioner's Handbook* (Toronto: Emond Montgomery Publications Limited, 2018), at page 47:

> What about when the state wants to access data on a computer without actually entering the place where the computer is located? More creative methods of remote data access are yet to be comprehensively considered in Canada courts, though there have been attempts in the United States for state actors to seek judicial authorization

croit les avoir détruits. L'ordinateur connecté à Internet sert de portail à une quantité presque infinie de données qui sont partagées entre différents utilisateurs et stockées presque n'importe où dans le monde. De même, depuis un ordinateur connecté à un réseau, les services de police et de renseignement peuvent avoir accès à des informations qui se trouvent dans d'autres appareils.

[23] Dans l'arrêt *R. c. Marakah*, 2017 CSC 59, [2017] 2 R.C.S. 608, au paragraphe 37, la Cour suprême du Canada a souligné que les conversations électroniques sont susceptibles de révéler une somme considérable de renseignements personnels. Le maintien d'un « "espace privé" » protégeant les renseignements personnels contre les intrusions de l'État est la raison d'être de l'article 8 de la Charte. Cet espace privé s'étend bien au-delà de l'appareil mobile d'une personne. En effet, il peut englober les conversations électroniques par lesquelles elle communique des renseignements personnels. Il est raisonnable de s'attendre à ce que les interactions privées, et non seulement le contenu d'un téléphone cellulaire à un moment précis, demeurent privées.

B. *Fouilles à distance*

[24] Grâce à un implant installé à distance, le Service peut intercepter [***] il est tout à fait possible qu'un implant soit installé sur un appareil dont un tiers innocent est propriétaire ou qu'il utilise. Cette possibilité devient très forte lorsque [***] est associée à un endroit public comme un café Internet.

[25] L'*amicus curiae* a avisé la Cour qu'au Canada, les précédents ayant trait aux conséquences juridiques de l'installation d'implants à distance sont peu nombreux, se référant à un passage de l'ouvrage de Gerald Chan et de Susan Magotiaux, *Digital Evidence : A Practitioner's Handbook* (Toronto : Emond Montgomery Publications Limited, 2018), page 47 :

> [TRADUCTION] Qu'arrive-t-il si l'État veut accéder à des données stockées sur un ordinateur sans pénétrer dans le lieu où il se trouve? Les tribunaux canadiens n'ont pas encore étudié de façon exhaustive certaines méthodes créatives permettant l'accès aux données à distance. Cependant, aux États-Unis, des intervenants étatiques ont cherché à

for offsite access through the use of programs delivered covertly to a target machine.

[26] In "Modern Technology and Privacy Rights: Leading Canadian and U.S. Case Law" (Ontario Bar Association Criminal Justice, Vol. 22, No. 10 (June 2013)), Assistant Crown Attorney Brock Jones refers to a case in which parole authorities were denied a warrant to search for breaches of a long-term supervision order. Mr. Jones offers the following comments, at page 8:

> The government's reliance on an IP address associated to emails sent and received from the presumed "target computer" lends itself to potential pitfalls. The person(s) sending the emails in question may have used "spoofing" software to disguise their true IP address, and therefore the installation of the Trojan software could target innocent computer users and their computers. The computer in question could also be in a public space such as a café or library. Installation of the spyware would potentially capture many innocent persons utilizing the computer for innocent purposes. The government's application would also permit real-time video surveillance via the computer's webcam. As such, the government must apply for a wiretap authorization, not a warrant. Future applications must address the court's concerns before a warrant would issue. [Emphasis added.]

[27] *In re Warrant to Search a Target Computer at Premises Unknown*, 2013 WL 1729765, at pages 3 and 4, United States Magistrate Judge Stephen W.M. Smith of the District Court for the Southern District of Texas, Houston Division, refused an application for a warrant to target a computer remotely. While the ruling must be understood within the unique legal context of that jurisdiction, Judge Smith asked a number of questions that are potentially germane to the present case:

> This "method" of software installation is nowhere explained. Nor does the Government explain how it will ensure that only those "committing the illegal activity will be … subject to the technology." What if the Target Computer is located in a public library, an Internet café, or a workplace accessible to others? What if the computer

obtenir des tribunaux l'autorisation d'obtenir un tel accès au moyen de logiciels installés secrètement dans un appareil visé.

[26] Dans son article « Modern Technology and Privacy Rights : Leading Canadian and U.S. Case Law » (L'Association du Barreau de l'Ontario Justice pénale, vol. 22, nº 10 (juin 2013, page 8)), le procureur adjoint de la Couronne Brock Jones fait allusion à une affaire où les autorités chargées des libérations conditionnelles n'ont pas pu obtenir un mandat de perquisition en vue de constater des violations d'une ordonnance de surveillance de longue durée.

> [TRADUCTION] En se fiant à une adresse IP liée aux courriels envoyés de l'« ordinateur cible » présumé ou qui lui sont parvenus, le gouvernement s'expose à tomber dans un piège. Quiconque envoie les courriels en question peut avoir utilisé un logiciel d'usurpation pour masquer sa véritable adresse IP. Par conséquent, l'installation du cheval de Troie peut se faire aux dépens d'utilisateurs innocents et de leurs appareils. L'ordinateur en question peut aussi se trouver dans un lieu public comme un café ou une bibliothèque. Ainsi, les activités anodines de nombreuses personnes innocentes pourraient être captées par le logiciel espion. L'application gouvernementale permettrait d'exercer une surveillance par l'entremise de la webcaméra de l'ordinateur, et ce, en temps réel. Par conséquent, le gouvernement doit demander une autorisation d'écoute électronique plutôt qu'un mandat. Les demandes futures doivent répondre aux préoccupations de la Cour, avant qu'un mandat puisse être décerné. [Non souligné dans l'original.]

[27] Dans *In re Warrant to Search a Target Computer at Premises Unknown*, 2013 WL 1729765, aux pages 3 et 4, le juge Stephen W.M. Smith de la Cour du district Sud du Texas, division de Houston, a refusé une demande de mandat visant un ordinateur à distance. Si la décision doit être interprétée dans le contexte propre à cette juridiction, il n'en reste pas moins que le juge Smith a posé des questions qui peuvent être pertinentes en l'espèce.

> [TRADUCTION] Cette « méthode » d'installation de logiciel n'est expliquée nulle part. En outre, le gouvernement n'explique pas comment il s'assurera que seules les personnes « qui mènent l'activité illégale […] seront visées par la technologie ». Que se passera-t-il si l'ordinateur visé se trouve dans une bibliothèque publique, dans un café

> is used by family or friends uninvolved in the illegal scheme? What if the counterfeit email address is used for legitimate reasons by others unconnected to the criminal conspiracy? What if the email address is accessed by more than one computer, or by a cell phone and other digital devices? There may well be sufficient answers to these questions, but the Government's application does not supply them. [Footnote omitted; emphasis added.]

[28] In "Beware of Government Agents Bearing Trojan Horses", (2015), 48 *Akron L. Rev.* 314: Issue 2, Article 4 at pages 345 to 347, Assistant Professor Brian L. Owsley of Texas Tech University Law School suggests that concerns of this nature may be addressed through a prior authorization process, and by putting protocols in place. In particular: (a) investigators must be barred from keeping third party information that is unrelated to the investigation; (b) investigators must distinguish between information that is relevant to the subject of the investigation on the targeted computer and non-relevant materials, such as personal photos and financial information that does not evidence any criminal activity; and (c) hard copies of irrelevant materials must be destroyed, and any electronic records must be deleted.

C. *Minimization Protocols*

[29] The destruction of data seized from innocent third parties is one way to limit the invasiveness of an electronic search, but it is not the only one. The warrant itself may minimize intrusion into the Charter rights and privacy interests of third parties.

[30] In *R. v. Thompson*, [1990] 2 S.C.R. 1111 (*Thompson*), the Supreme Court of Canada considered a "'resort to'" clause in an authorization to intercept private communications. The clause would authorize the police to monitor communications from a location the target may "'resort to'", in this case a pay telephone available to the public. Justice John Sopinka said the following, at pages 1143–1144:

> Internet ou dans un lieu de travail accessible à d'autres personnes, ou s'il est utilisé par des membres de la famille ou des amis qui n'ont rien à voir avec l'activité illégale? Qu'arrivera-t-il si la fausse adresse de courriel est utilisée à des fins légitimes par des personnes qui n'ont pas partie liée au complot criminel? Et si l'adresse de courriel est consultée depuis plus d'un ordinateur ou au moyen d'un téléphone cellulaire et d'autres appareils numériques? S'il existe des réponses satisfaisantes à ces questions, le gouvernement ne les donne pas dans sa demande. [Note en bas de page omise; non souligné dans l'original.]

[28] Dans l'article « Beware of Government Agents Bearing Trojan Horses » ((2015), 48 *Akron L. Rev.* 314, nº 2, article 4, aux pages 345 à 347), Brian L. Owsley, professeur adjoint à l'école de droit de l'Université Texas Tech, laisse entendre que les préoccupations de cette nature pourraient être atténuées grâce à un processus d'autorisation préalable et à la mise en place de protocoles. En particulier, a) il faut interdire aux enquêteurs de conserver des informations de tiers non liées à l'enquête; b) les enquêteurs doivent, dans les informations stockées sur l'ordinateur visé, établir une distinction entre les informations qui concernent leur cible et les documents non pertinents, par exemple des photos personnelles et des données financières sans lien avec des activités criminelles; c) il est impératif de détruire les copies papier des documents non pertinents et de supprimer tout fichier électronique.

C. *Protocoles de réduction au minimum des répercussions*

[29] La destruction des données obtenues de tiers innocent dans le cadre d'une fouille n'est qu'une des manières de limiter le caractère intrusif de la fouille. Le mandat lui-même peut minimiser l'empiètement sur les droits garantis par la Charte et sur le droit des tiers au respect de leur vie privée.

[30] Dans l'arrêt *R. c. Thompson*, [1990] 2 R.C.S. 1111 (*Thompson*), aux pages 1143 et 1144, la Cour suprême du Canada a étudié, dans une autorisation d'intercepter les communications privées, une disposition sur les « "endroits fréquentés" » qui autoriserait la police à surveiller les communications effectuées à un endroit que la cible est susceptible de fréquenter, dans ce cas un téléphone public. Selon le juge John Sopinka :

> In any authorization there is the possibility of invasion of privacy of innocent third parties. For instance a wiretap placed on the home telephone of a target will record communications by other members of the household. This is an unfortunate cost of electronic surveillance. But it is one which Parliament has obviously judged is justified in appropriate circumstances in the investigation of serious crime.
>
> In my view, in some cases the possibility of invasion of privacy of innocent persons may become so great that it requires explicit recognition along with the interests of the investigation of crime. A "resort to" clause creates just this possibility if among the places resorted to are telephones frequently used by the general public or other such places. I do not mean to suggest that there should be a constitutional prohibition of intercepting communications at places frequented by the public; in that case drug importing conspiracies could virtually insulate themselves from perhaps the only effective investigative technique against them merely by using public places to conduct their business.

[31] The Supreme Court did not find the "resort to" clause to be unlawful under the relevant provisions of the *Criminal Code* [R.C.S., 1985, c. C-46], and the authorizations were found to be valid. However, given the extent of the invasion of privacy authorized, a total absence of any protection for the public created a potential for carrying out searches and seizures that were unreasonable. Justice Sopinka explained, at pages 1145–1146:

> Interceptions which were made pursuant to these authorizations, which were simply fishing expeditions and not based on reasonable and probable grounds for believing the target would be utilizing the pay telephones at the time, were, in my opinion, unreasonable. In most instances, it would be preferable to have actual physical surveillance of the public telephone to ensure that it is being used by the target. This is said to be normal police practice. I am, however, in agreement with Martin J.A. and Professor Stanley A. Cohen that to make this an absolute requirement would impose too heavy a burden on Canadian law enforcement officials.

[32] Although *Thompson* was decided almost three decades ago when the Internet was still in its infancy, the

> Dans toute autorisation, il peut y avoir atteinte à la vie privée de tiers innocents. Par exemple, le dispositif d'écoute installé sur le téléphone de la résidence d'une cible enregistrera les communications des autres occupants de la maison. C'est l'un des inconvénients malheureux de la surveillance électronique. Mais il s'agit d'un inconvénient que le Parlement a évidemment estimé justifié dans des circonstances appropriées au cours d'une enquête portant sur un crime grave.
>
> À mon avis, la possibilité d'atteinte à la vie privée de personnes innocentes peut prendre des proportions tellement importantes dans certains cas qu'elle doit être reconnue expressément au même titre que les intérêts qu'il y a à enquêter sur un crime. Une clause des « endroits fréquentés » est justement à l'origine de cette possibilité si parmi les lieux fréquentés on retrouve des téléphones publics utilisés par le grand public ou d'autres lieux semblables. Je ne dis pas qu'il devrait y avoir une interdiction constitutionnelle d'intercepter les communications dans les lieux fréquentés par le public; dans ce cas, les auteurs de complots en vue d'importer des stupéfiants pourraient pratiquement se soustraire à ce qui est peut-être le seul moyen d'enquête efficace contre eux simplement en utilisant des lieux publics pour faire leurs affaires.

[31] La Cour suprême a conclu que la disposition sur les « endroits fréquentés » ne contrevenait pas aux dispositions applicables du *Code criminel* [L.R.C. (1985), ch. C-46] et que, partant, les autorisations étaient valides. Toutefois, compte tenu de l'ampleur de l'atteinte autorisée à la vie privée, l'absence totale de toute mesure de protection du public entraînait la possibilité que soient effectuées des fouilles, des perquisitions ou des saisies abusives. Selon le juge Sopinka (aux pages 1145 et 1146) :

> À mon avis, les interceptions effectuées conformément à ces autorisations, qui étaient simplement des recherches à l'aveuglette non fondées sur des motifs raisonnables et probables de croire que la cible utiliserait alors les téléphones publics, étaient abusives. Dans la plupart des cas, il serait préférable qu'il y ait une véritable surveillance physique du téléphone public pour s'assurer qu'il est utilisé par la cible. On dit qu'il s'agit de la pratique policière normale. Je partage cependant l'opinion du juge Martin et du professeur Stanley A. Cohen que d'en faire une exigence absolue imposerait un fardeau trop lourd aux responsables de l'application de la loi canadienne.

[32] Ce principe demeure valable et s'applique en l'espèce, même si l'arrêt *Thompson* a été rendu il y a

principle remains valid and applicable here. Minimization conditions in a warrant may not be required in every case, but they may be required in some cases depending on the extent of the potential invasion of the privacy of innocent third parties.

[33] More recently, the Supreme Court of Canada decided in *Vu* that a warrant was needed to explicitly authorize the search of a computer. The police could not rely on a warrant to search the residence from which the computer was seized.

[34] The Supreme Court in *Vu* proposed, in effect, to treat computers as if they were a separate place of search necessitating distinct prior authorization. However, Justice Thomas Cromwell was not persuaded that section 8 of the Charter requires that the manner of searching a computer always be spelled out in advance. He reached this conclusion for two reasons. First, the manner of search in a criminal investigation is generally reviewed after the fact, which is better suited to developing new rules about how searches should be conducted than the *ex parte* procedure by which warrants are issued. Second, requiring search protocols to be imposed in advance of the search would add significant complexity and practical difficulty at the authorization stage. Attempts to impose search protocols during the authorization process risk creating blind spots in an investigation, undermining the legitimate goals of law enforcement that are recognized in the pre-authorization process. These problems are magnified by rapid and constant technological change.

[35] While search protocols may not be constitutionally required in all cases, authorizing justices must assure themselves that the warrants they issue fulfil the objectives of prior authorization. They also have the discretion to impose conditions to ensure they do. Justice Cromwell observed that an authorization might include directions concerning the manner of search. He did not foreclose the possibility that our developing understanding of computer searches and changes in technology may make it

presque 30 ans, lorsque l'Internet n'en était qu'à ses balbutiements. Il se peut que des conditions prévoyant la réduction au minimum des répercussions ne soient pas nécessaires dans tous les cas; cela dépend de l'ampleur de l'atteinte possible à la vie privée de tiers innocent.

[33] Récemment, dans l'arrêt *Vu*, la Cour suprême du Canada a statué que la fouille d'un ordinateur doit être autorisée explicitement par un mandat. Partant, la police ne pourrait pas s'appuyer sur un mandat l'autorisant à perquisitionner le domicile où elle a saisi l'ordinateur.

[34] Dans l'arrêt *Vu*, la Cour suprême propose en effet de traiter un ordinateur comme un lieu distinct dont la fouille requiert en soi une autorisation préalable. Toutefois, le juge Thomas Cromwell n'était pas persuadé que l'article 8 de la Charte requiert que la manière de fouiller un ordinateur soit toujours précisée à l'avance. Il a appuyé sa conclusion sur deux motifs. Premièrement, la manière dont une fouille a été effectuée dans le cadre d'une enquête criminelle fait généralement l'objet d'un contrôle a posteriori, démarche plus propice à l'élaboration de nouvelles règles sur la façon d'effectuer des fouilles que ne l'est la procédure *ex parte* de délivrance des mandats. Deuxièmement, le fait d'exiger que soient imposés des protocoles de perquisition avant l'exécution de la fouille rendrait vraisemblablement l'étape de l'autorisation beaucoup plus complexe, en plus de créer des difficultés d'ordre pratique. Toute tentative d'imposer des protocoles de perquisition à l'étape de l'autorisation risque de créer des angles morts dans une enquête et de contrecarrer les objectifs légitimes de l'application de la loi dont tient compte le processus d'autorisation préalable. Ces problèmes sont amplifiés par l'évolution rapide et constante de la technologie.

[35] S'il est possible que des protocoles de fouille ne soient pas constitutionnellement requis en toutes circonstances, le juge saisi de la demande d'autorisation doit tout de même s'assurer que les mandats qu'il décerne répondent aux objectifs de la procédure d'autorisation préalable. Il possède en outre le pouvoir discrétionnaire d'imposer des conditions à cette fin. Le juge Cromwell a souligné que l'autorisation peut comporter des directives sur la manière de procéder à la fouille et il n'a pas

appropriate to impose search protocols in a broader range of cases in the future (*Vu*, at paragraph 62).

[36] The *amicus curiae* notes that there are a number of important differences between the use of warrant powers by the police and those employed by CSIS. One of the rationales provided by Justice Cromwell in *Vu* for not requiring search protocols in all warrants was that the reasonableness of the search was best examined after the fact. However, very few warrants issued to the Director of CSIS are examined after the fact, in large measure because they are unlikely to result in criminal charges. Justice Cromwell's concern about complexity and inadvertently limiting the effectiveness of investigation does not arise here. The affiants have proposed a workable protocol which is currently being used on an informal basis.

[37] Given the extent of the potential invasion of the privacy of innocent third parties, the Attorney General of Canada and the *amicus curiae* agree that minimization conditions are required in warrants that authorize the remote installation of implants on devices. The *amicus curiae* has proposed that, consistent with the Chief Justice's recommendation at the *en banc* presentation on December 15, 2017, the survey stage be made mandatory before full data collection commences. He also recommends that the data obtained at the survey stage be strictly limited to the categories described in paragraphs 10 and 11 of these reasons for order.

[38] With these modifications, I am satisfied that the searches to be conducted under warrants requested by the Director of CSIS are reasonable. The search protocols are sufficiently robust to safeguard the Charter and privacy rights or interests of innocent parties. The warrants should therefore be granted.

écarté la possibilité que l'amélioration des connaissances en matière de fouilles d'ordinateurs ainsi que l'évolution des technologies puissent finir par justifier l'imposition de protocoles de perquisition dans un éventail de situations élargi (*Vu*, au paragraphe 62).

[36] L'*amicus curiae* souligne qu'il existe des différences importantes entre les pouvoirs prévus par les mandats qu'exécute la police et ceux qu'exécute le SCRS. Dans l'arrêt *Vu*, le juge Cromwell soutient qu'il n'y a pas lieu que tous les mandats comportent un protocole de fouille parce que, notamment, il est préférable d'examiner le caractère raisonnable de la fouille a posteriori. Toutefois, très peu de mandats décernés au directeur du SCRS font l'objet d'un tel examen, en grande mesure parce qu'il y a peu de chances qu'ils donnent lieu à des accusations criminelles. La préoccupation du juge Cromwell au sujet de la complexité de l'enquête et de la possibilité d'en miner l'efficacité par inadvertance est infondée en l'espèce. Les déposants ont proposé un protocole viable, actuellement utilisé à titre informel.

[37] Compte tenu de l'ampleur de l'atteinte éventuelle à la vie privée de tiers innocents, la procureure générale du Canada et l'*amicus curiae* conviennent que les mandats qui autorisent l'installation à distance d'implants dans des appareils doivent comporter des mesures de réduction au minimum des répercussions. L'*amicus curiae* a proposé que l'étape de l'analyse soit rendue obligatoire avant que la collecte de données puisse commencer, comme l'a recommandé le juge en chef lors de l'exposé entendu en formation plénière le 15 décembre 2017. L'*amicus curiae* a aussi recommandé que les données obtenues à l'étape de l'analyse se limitent strictement aux catégories énumérées aux paragraphes 10 et 11 des présents motifs.

[38] Moyennant l'apport des modifications susmentionnées, je suis convaincu du caractère raisonnable des fouilles qui seront effectuées en vertu des mandats demandés par le directeur du SCRS. Les protocoles de fouille sont suffisamment rigoureux pour protéger les droits garantis par la Charte et le droit des tiers innocents à la protection de leur vie privée. Partant, il y a lieu de décerner les mandats.

V. Conclusion

[39] The warrants that authorize the remote installation of an implant on any device, including one that belongs to or is used by an innocent third party, may only be issued with the following search protocols:

1. Where an implant is remotely installed on a device [***] a survey of the device must be performed prior to intercepting communications and obtaining the information described in the warrants.

2. The data obtained at the survey stage must be limited to those described in paragraphs 10 and 11 of these reasons for order.

3. A designated Service employee must review the data obtained at the survey stage and determine whether there are reasonable grounds to believe that the device is (a) a portable device belonging to or used by the subject of investigation; or (b) a computer holding information that may be obtained pursuant to a general intercept and search warrant.

4. If either condition 3(a) or (b) is met, then the survey information may be retained and full interception and collection from the device may commence.

5. If neither condition 3(a) or 3(b) is met, then the survey information must be destroyed as soon as reasonably practicable, but no later than six months from the date it was obtained. No further use of the survey information may be made.

V. Conclusion

[39] Tout mandat autorisant l'installation à distance d'un implant sur tout appareil, y compris un appareil dont un tiers innocent est propriétaire ou qu'il utilise doit, pour être décerné, comporter les protocoles de fouille suivants :

1. Tout appareil dans lequel un implant a été installé à distance [***] fait l'objet d'une analyse avant que commencent l'interception des communications et l'obtention des informations mentionnées dans les mandats.

2. Les données obtenues à l'étape de l'analyse se limitent aux catégories énumérées aux paragraphes 10 et 11 des présents motifs.

3. Après examen des informations obtenues à l'étape de l'analyse, un employé du Service désigné détermine s'il existe des motifs raisonnables de croire que l'appareil est a) un appareil portable dont la cible est propriétaire ou qu'elle utilise ou b) un ordinateur qui contient des informations pouvant être obtenues en vertu du mandat sur les interceptions générales et les fouilles.

4. Si l'appareil respecte l'une ou l'autre des conditions 3a) et b), les informations issues de l'analyse peuvent être conservées, et l'interception et la collecte visant l'appareil peuvent commencer.

5. Si ce n'est pas le cas, les informations issues de l'analyse sont détruites dès qu'il est matériellement possible de le faire et, au plus tard dans les six mois suivant l'obtention, sans être autrement utilisées.